THE STATE OF INTEROPERABLE COMMUNICATIONS PART I, II AND III

HEARING

BEFORE THE

SUBCOMMITTEE ON EMERGENCY PREPAREDNESS, SCIENCE, AND TECHNOLOGY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

FEBRUARY 15, 2006, MARCH 1, 2006, and APRIL 25, 2006

Serial No. 109–62

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE

36–399 PDF WASHINGTON : 2007

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

DON YOUNG, Alaska
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
CHRISTOPHER SHAYS, Connecticut
JOHN LINDER, Georgia
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
JIM GIBBONS, Nevada
ROB SIMMONS, Connecticut
MIKE ROGERS, Alabama
STEVAN PEARCE, New Mexico
KATHERINE HARRIS, Florida
BOBBY JINDAL, Louisiana
DAVE G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
CHARLIE DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida

SUBCOMMITTE ON EMERGENCY PREPAREDNESS, SCIENCE, AND TECHNOLOGY

DAVE G. REICHERT, Washington, *Chairman*

LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
ROB SIMMONS, Connecticut
MIKE ROGERS, Alabama
STEVAN PEARCE, New Mexico
KATHERINE HARRIS, Florida
MICHAEL MCCAUL, Texas
CHARLIE DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
PETER T. KING, New York *(Ex Officio)*
BILL PASCRELL, JR., New Jersey
LORETTA SANCHEZ, California
NORMAN D. DICKS, Washington
JANE HARMAN, California
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

CONTENTS

THE STATE OF INTEROPERABLE COMMUNICATIONS: PERSPECTIVES FROM THE FIELD PART I

Wednesday, February 15, 2006

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON EMERGENCY PREPAREDNESS,
SCIENCE AND TECHNOLOGY,
Washington, DC.

The subcommittee met, pursuant to call, at 10:00 a.m., in Room 311, Cannon House Office Building, Hon. Dave Reichert [chairman of the subcommittee] presiding.

Present: Representatives Reichert, Dent, Jindal, Pascrell, Thompson, Harman, Lowey, Norton, Christensen, and Etheridge.

Mr. REICHERT. [Presiding.] Good morning. The Committee on Homeland Security, Subcommittee on Emergency Preparedness, Science and Technology will come to order.

The subcommittee will hear testimony today on perspectives from the field on the state of interoperable communications.

I would first like to welcome our witnesses and thank them for taking time out of their busy schedules to be with us today. Thank you very much.

I would also like to ask unanimous consent to allow Mr. Jindal to be a part of our panel this morning and be allowed to question the witnesses.

Without objection.

Good morning. Let me first welcome our distinguished panel and thank you all for being here to share your thoughts on the issue of great personal and professional importance to me: The problem of achieving and maintaining interoperable emergency communications.

I would like to be really, very, very blunt here: It is intolerable to me that our nation's law enforcement, fire service and emergency medical personnel still confront many of the same emergency communications problems that I did as a rookie cop more than 34 years ago.

It is intolerable to me that even with the rapid pace of technological and innovation and the vast amounts of money dedicated to improving emergency communication, our nation's first responders still experience difficulty communicating with one another on demand, in real time when needed.

Until the events of September 11, 2001, many people just simply assumed that first responders from different disciplines and jurisdictions could communicate with one another. Unfortunately, that was not the case then. And as demonstrated by the inadequate response to Hurricane Katrina, it is not the case even now.

The inability of police, fire, emergency medical services, public works, utilities and health case workers to communicate with one another effectively, may have even led to the loss of many lives in New Orleans and the Gulf states. The status quo is unacceptable.

Our local police, fire and emergency medical service professions are our nation's first line of prevention, preparedness, response and recovery. And effective communication is absolutely essential to their mounting a well-coordinated response, whether manmade or natural. Indeed, first responders and federal, state and local officials cannot establish meaningful command and control in the absence of a functioning communication system.

Without the ability to receive timely reports from the field, the incident commander may have difficulty establishing situational awareness. Without the ability to issue instructions to first responders in the field, the operations chief cannot direct resources and personnel to areas where they are most needed. And without the ability to call for help, citizens cannot reliably seed medical and other emergency assistance. In other words, effective communication is essential for the right people to make the right decisions at the right time.

The message is worth repeating: To mount an effective emergency response requires timely and accurate information so that the right people may make the right decisions at the right time.

As I previously said, I have firsthand understanding and experience and an appreciation for this problem. Suffice it to say, I have faced the perils of life and death decision-making in my law enforcement career, and as sheriff of King County in Seattle, I have provided the safest possible environment for those that served in my office.

But, sadly, inadequate emergency communications sometimes stood in my way. For example, the regional radio communications system in King County, in the Seattle area, which served all 49 governments in the county, suffered terrible interference.

The proliferation of cell phone towers overpowered and disrupted the deputies' ability to receive their radio signals, thus jeopardizing their safety. As sheriff, I took immediate remedial action to redress that particular situation. But now as a Member of Congress and chairman of this subcommittee, I have a forum through which I intend to solve this larger communication problem across our country.

While the recently enacted Deficit Reduction Act included a necessary initial step of freeing up much needed spectrum and established a $1 billion interoperable grant program, interoperable communications is about much more than just spectrum and money. It was about the need for strong leadership, effective communication, adequate planning and a management system that worked.

Today is the first in a series of hearings that will be scheduled in the future to highlight the issues and perspectives of the various experts which you are all here as members of and I know serve on

the front lines. Sort of where the rubber meets the road, kind of, is what we need to hear.

In the successive hearings, the subcommittee will hear the perspectives of state and local officials, federal officials who administer interoperable grant programs and other activities and experts in the field of emergency communications technology.

And, again, I want to thank the witnesses for their testimony today.

The Chair now recognizes the ranking minority member of the subcommittee, the gentleman from New Jersey, Mr. Pascrell.

Mr. PASCRELL. Thank you, Mr. Chairman, and thank you for holding this series of hearings. And as you know, I must apologize, I have three things going on at the same time, but the Ranking Member is here and obviously will carry on as will other members.

It goes without saying that this an issue of utmost urgency. My profound hope is that this subcommittee, with the leadership of my friend, Chairman Reichert, will have as its legacy a lasting solution for the communications problem.

Indeed, I am heartened by the chairman's commitment to hold these hearings in anticipation of bipartisan legislation, which we have already started to look at, that will improve the communication capabilities of emergency responders. I can assure all of you who are testifying today, we mean business.

When the 9/11 Commission released its final report, it found that the inability of our first responders to talk with each other and their commanders resulted in a loss of life. The 9/11 Commission identified the need for more spectrum as crucial to assist emergency responders in communicating during an emergency such as a terrorist attack or a hurricane.

But the 9/11 Commission in this regard, at least, identified a problem that has been in existence for decades, and it identified a problem that many policy makers have known about for some time.

In 1996, Congress, asked a blue ribbon committee, the Public Safety Wireless Advisory Committee, to examine the issues of interoperable communications. It concluded 10 years ago that public safety agencies did not have sufficient radio spectrum to do their jobs.

This is nothing new to you. You are the front lines, we thank you for your service, and here we are again.

The committee is supposed to have congested channels on radio frequencies cleared on the fifth anniversary date of the release of the report. Five years later, on September 11, 2001, the spectrum identified was still not available for public safety use in most of the nation.

In 2002, the National Task Force on Interoperability convened several meetings with various national associations representing public safety officials to discuss the challenges of interoperable communications. They explicitly identified the key challenges that must be addressed if we are to move forward.

For example, incompatible and aging equipment, limited funding from the federal government, fragmented planning, in general, lack of coordination and cooperation from all different stakeholders, as well as, of course, insufficient radio spectrum. And I might add, Trooper Perry, I did read through all of your testimony, by the

way, and again apologize for having to leave soon. But I did read yours, and I want to just quote something that you did say in your presentation: "The lack of common standards among vendors continues to present difficulties of interconnection."

Now, I am certainly not an expert on interoperability, but it is pretty logical here, if vendors of equipment and software received tax-supported dollars from state, counties and municipal governments, they must be held accountable so that their products will create optimal technologies compatible with other vendors' systems. That is pretty logical to us, but it is not happening.

So they have known about the problems, and many have explored the possible remedies that we should undertake. Yet here we sit after 9/11, after Hurricane Katrina wondering why no real progress has been made, not only in this area but in other areas.

And I think it is fair to add that I believe the current administration has provided very little leadership. The President's fiscal year 2007 budget requests no funds for grants to enhance interoperability. I want that to set in this morning. Nada. Zero.

The President's fiscal year 2007 budget proposed to eliminate the COPS Interoperability Grant Program, which is charged with awarding technology grants to law enforcement agencies for the purpose of enhancing interoperability and information sharing. The President zeroes out this program after it was significantly cut in fiscal year 2006 budget. It was funded at $10 million, down from $99 million in the fiscal year 2005 budget.

The administration justifies its proposed elimination of COPS interoperability grants on the ground that the program is redundant with the efforts of the Department of Homeland Security. The Department does not have a dedicated interoperability grant program, however.

Now, who are we kidding here?

We stand behind the executives whenever they get their pictures taken, and you guys and gals are there all the time, and it is time—if the gig is up, the gig is up. If we mean business, let's do something about it. If we do not mean business, then we will have charades, time for more charades. I do not think this chairman wants a charade. I am convinced that he does not.

This has nothing to do with partisan politics either. This administration does not get it. I do not know what party they belong to, to be very honest with you.

The President's budget proposes a modest $3.5 million increase for the Office of Interoperability and Compatibility in the 2007 budget. This increase is far less than what is necessary to remedy the weaknesses that were evident with the glaring failure of emergency communication in Katrina and Rita.

This slight increase is far from what SAFECOM, with only four to seven full-time employees, needs to accelerate the standards and the development of interoperable communications equipment.

We are long past the point where we in Washington pay lip service to the problem. I know my chairman feels the same way.

Finally, I would like to add that as we move forward and work toward achieving interoperability, we must realize that we are facing basic operability issues as well. Past domestic and international

instances, whether manmade or natural disasters, have shown that our nation's communications systems are closely tied together.

We have seen that one storm can overload or completely damage our landline-based communications systems. Wireless networks, land-based radio communications systems simultaneously. We need to continue to work together to determine how we can be prepared if an event takes all our terrestrial communications systems out at once.

Indeed, we have some very serious responsibilities before us and look forward to working closely with Chairman Reichert to help propose serious solutions to these serious problems.

And I might add, Mr. Chairman, that I am glad to see that we are going to have the FCC before us, and all hell is going to break out, I am going to tell you that, when they get here. As you well know, we have a history.

So I want to commend you for the floor hearings you put together. This is no easy task, and it is not going to be pleasant, it is not going to be a day at the beach, but we are going to get something accomplished. Thank you.

Thank you, Mr. Chairman.

Mr. REICHERT. Thank you. Thank you, Mr. Pascrell. It is a good thing there is a sheriff in the house. We do not want all hell to break loose.

[Laughter.]

The Chair now recognizes the ranking minority member of the full committee, the gentleman from Mississippi, Mr. Thompson.

Mr. THOMPSON. Thank you very much, Chairman Reichert and Ranking Member Pascrell. I want to associate myself with your comments. I agree with them wholeheartedly.

But, also, as you know, this is the first of four hearings that we will hold on this issue, on the challenges of achieving interoperability during times of emergency.

As a former volunteer firefighter, I can personally attest to the important communications that first responders need during emergencies. It can mean the difference between life and death. It is deeply unsettling that even after the devastating Oklahoma bombing, the 9/11 attacks, the London and Madrid bombings and the catastrophic devastation of Hurricanes Katrina and Rita that interoperability communications remains a rainbow at the end of the storm. Everyone claims to see it in the horizon, but no one has been able to find a magical interoperable pot of gold at the other end.

The 9/11 communications report made it clear that interoperable communications is critical, yet the colossal communications challenges during Hurricane Katrina was a stinging indictment of Congress' to lead on a very critical issue.

I look forward to the testimony of the witnesses here today. I am also looking forward to the subsequent hearings on the roles of state and local government, the role of federal agencies in the state and impact of technology in the area of interoperable emergency communications.

The ultimate goal is to produce clear legislation that expedites and facilitates the delivery of emergency communications systems to those who need it most. It is not enough to make lofty speeches

that fail to give clear directives. It is not enough to support our first responders and yet shortchange them by improperly funding the critical programs that funds the emergency communication systems they need.

I, therefore, welcome the spirit of bipartisan, Mr. Chairman, in ultimately coming up with a piece of legislation that can fix this problem so that once and for all those individuals who are tasked with the responsibility of helping in time of need can in fact do their job and communicate with each other.

Thank you, and I look forward to the testimony today.

I yield back the balance of my time.

Mr. REICHERT. Other members of the committee are reminded that opening statements may be submitted for the record.

We are pleased to have a distinguished panel of witnesses with us today. First, we have Trooper Casey L. Perry of the Wisconsin State Patrol and chairman of the National Troopers Coalition. We also have with us today Mr. Tim Bradley, senior deputy state fire marshal for the North Carolina Office of State Fire Marshal and a member of the National Volunteer Fire Council; Ms. Diane Linderman, director-at-large of American Public Works Association; Mr. William Moroney, president and chief executive officer of the United States Telecom Council; and Dr. William Pinsky, executive vice president and chief academic officer of the Ochsner Clinic Foundation and a member of the American Hospital Association's Committee on Health Preparedness.

Let me remind the witnesses that their entire witness statement will appear in the record. We ask that due to the number of witnesses on our panel today that you strive to limit your comments to no more than 5 minutes.

The Chair now recognizes Trooper Perry.

First, before we go to the first witness, I would ask Mr. Jindal to introduce the gentleman from Louisiana.

Mr. JINDAL. Thank you, Mr. Chairman. I want to thank you and the other members for allowing me to come and sit with my colleagues on the subcommittee. I also want to thank you for holding this hearing. You are obviously uniquely qualified to talk about the issue of interoperability.

I certainly share my colleagues' frustrations. Having been through Hurricanes Katrina and Rita, we saw firsthand in Louisiana the difficulties caused by the lack of interoperable communications, this even after the fact the federal government spent billions of dollars toward interoperable communications. My colleagues have pointed out this has been a challenge not only since 9/11 but well before that.

It is my privilege to introduce not only a distinguished member of this panel before us but also an individual who was on the ground during Hurricane Katrina. Dr. Pinsky serves at the Ochsner Clinic Foundation or the hospital operated by the Ochsner Clinic Foundation.

I went of tell you a little bit about Ochsner and why it is so important we are hearing from Dr. Pinsky today. Ochsner's is one of only three hospitals in the greater New Orleans area that was able to stay open continuously through Hurricane Katrina. Despite the lack of power, despite being surrounded by flooded waters, they

were able to keep their doors open and to provide critical services for the people of the greater New Orleans area.

They are also one of three graduate medical education programs in the area and the only one that continues to operate at full capacity. So they were serving a critical role, and since the hurricane they have not closed their doors for one minute, and I think they need to be recognized and applauded for this heroic effort.

Dr. William Pinsky is the executive vice president, the chief academic officer of the foundation. He is responsible for all of the professional medical education and research programs. He received his medical degree from St. Louis University in 1973 following his training in pediatrics and pediatric cardiology at the Baylor College of Medicine.

Dr. Pinsky pursued a career in academic pediatric cardiology, served on the faculties at Baylor, the Baylor College of Medicine, the University of Nebraska, Tulane University and Wayne State University.

We are very pleased to have him here.

I will add, not only am I proud of the work they have done, my son is actually a patient at Ochsner, so I can say firsthand they do an excellent job for our community.

Thank you, Mr. Chairman.

Mr. REICHERT. Thank you, Mr. Jindal.

Mr. Etheridge, you have an introduction to make.

Mr. ETHERIDGE. Thank you, Mr. Chairman, and I am pleased to say a word for my friend, Tim Bradley, and welcome him to this subcommittee hearing today.

Tim is a senior deputy fire marshal for the state of North Carolina. He also serves as the state fire training director, which, as you know, is important as well. He is well-qualified to talk about state interoperable communications from the perspective of the first responder. Let me just say why.

He began his career with the Mebane Volunteer Fire Department, including 7 years as chief. He continues to serve as volunteer assistant chief even today. During his 32 years of public service, he has been a certified fire rescue instructor, fire arson investigator, life safety educator and hazardous material responder. So he has had a pretty good broad base, and so I look forward to his comments today.

You know, good interoperable communications are critical, as you well know, Mr. Chairman, to success in a response, and I was proud to join my colleague, Representative Harman in the HERO Act, but I am dismayed that the administration's foot-dragging in interoperable equipment. The President, as you have already heard, zeroed out the few programs that help local and state responders obtain communications technology, which I think is critical.

And the American people have a right to expect their national leaders to provide all the necessary means for their safety and security. And we should no longer tolerate negligence in the need for interoperable equipment now more than 4 years after 9/11 terrorist attack. Our first responders should not have to struggle to answer that famous TV commercial: "Can you hear me now?"

Thank you, and I yield back the balance of my time.

Mr. REICHERT. Thank you, Mr. Etheridge.
The Chair now recognizes Trooper Perry.

STATEMENT OF CASEY PERRY, CHAIRMAN, NATIONAL TROOPERS COALITION

Mr. PERRY. Good morning, Chairman Reichert, Ranking Member Pascrell and distinguished committee members. I am Casey Perry, chairman of the National Troopers Coalition, representing our nation's state troopers. It is both an honor and a privilege to be before this committee today in order to testify on state troopers' thoughts, ideas and concerns. I will share with you my experiences as users from the field who provide service and security to our citizens.

To begin, I would like to thank our members of Congress for their support to the Department of Homeland Security. I have served 3 years in the United States Army and 27 years as a Wisconsin state trooper. Throughout my career I have consistently confronted obstacles in cooperation and trust between the various layers of government and discipline of emergency services.

I am pleased to report, however, that since the creation of the Department of Homeland Security, we have made great strides in both trust-building and information sharing. During the past 2 years, I have attended various programs and conferences hosted by the Department of Homeland Security, Department of Justice and Office of Justice Assistance.

My experience has been as the delegates debate potential solutions to address the problems we face, the age-old failure continues between states, counties and municipal rights, as well as with the disciplinary of emergency medical services, fire, law enforcement and emergency government. Each entity resists losing their share of control.

This is the underlying root of the problems we face today. We cannot address communication interoperability without first addressing the problems in the current power structure as we continue to waste our tax dollars.

The government, in serving as the parental figure, has to hold the children and it has told the children to be nice to their brother and sister but has failed as a parent in gaining compliance.

The parent needs to now withhold the children's allowance, or in this case federal grant money, until they learn to cooperate with each other. We need to overcome the political issues across our jurisdictions to build a communications platform that will serve each partner equally. The cost-building of such a program is not a one-time investment. It will require ongoing investments.

Therefore, federal grant monies need to come with strings attached. States must be held accountable in creating a communications network that is a dedicated channel and/or shared channel capability for EMS, fire, law enforcement and emergency government, which will serve their entire state, allowing each county and municipal government full access.

States redistributing federal grant money to county and municipal governments must ensure the money is spent on compatible equipment and software to interface with the statewide platform.

The lack of common standards among vendors continue to present difficulties in interconnection. If vendors of equipment and

software receive tax-supported dollars from states, counties or municipal governments, they must be held accountable. So their products will create optimal technologies compatible with other vendors' systems.

Being on the front line, so to speak, troopers and other law enforcement officers throughout our nation rely on communication each and every day. Agencies must provide equipment that will allow our law enforcement officers to communicate with one another along with other disciplines of EMS, fire, emergency government.

As communication equipment users, we count on other law enforcement jurisdictions, EMS and fire several times a day during the regular course of our duty. If we address the issue of interoperability at the basic level here, on the front line, during these daily occurrence, we will have addressed a number of issues regarding the localized emergency response, services involving multiple intrajurisdictions, planned events, including athletic events, conferences and conventions and regional incident management of natural and manmade disasters.

In closing, it is my assessment that currently federal tax dollars are not being allocated, managed or spent efficiently. Furthermore, there are no mechanisms in place to ensure accountability. Therefore, the lack of such coordination among our federal programs creates confusion and duplication of equipment and software that the end users contend with on a daily basis.

I would be happy to answer any of your questions after the other panel members have a chance to provide testimony, and I will be more than happy to provide personal experiences related to my testimony.

Thank you.

[The statement of Mr. Perry follows:]

PREPARED STATEMENT OF CASEY PERRY

WEDNESDAY, FEBRUARY 15, 2006

Good morning Chairman Reichert, Ranking Member Pascrell and distinguished Committee Members. I am Casey Perry, Chairman of the National Troopers Coalition (NTC), representing our nation's state troopers. It is both an honor and a privilege to appear before this committee today in order to testify on state troopers' thoughts, ideas, and I will share with you our experiences as users from the field who provide service and security to our citizens.

To begin, I would like to thank our Members of Congress for their support of the Department of Homeland Security. I served three years in the U.S. Army and the past 27 years as a Wisconsin State Trooper. Throughout my career I have consistently confronted obstacles in cooperation and trust between the various layers of government and disciplines of emergency services. I am pleased to report, however, that since the creation of the Department of Homeland Security we have made great strides in both trust-building and information sharing.

During the past few years I have attended various programs and conferences hosted by the Department of Homeland Security, Department of Justice, and the Office of Justice Assistance. My experience has been that as the delegates debate potential solutions to address the problems we face, the age-old barriers continue between states, counties, and municipal rights, as well as with the discipline areas of emergency medical service, fire, law enforcement, and emergency government. Each entity resists losing their share of control. This is the underlying root of the problems we face today. We cannot address communication interoperability without first addressing the problems in the current power structure or we will continue to waste our tax dollars. The govemment, in serving as a parental figure, has told the children to be nice to their brother and sister but has failed as a parent in gaining com-

pliance. The parent now needs to withhold its children's allowance (or in this case federal grant money) until they learn to cooperate with each other.

We need to overcome the political issues across our jurisdictions to build a communication platform that will serve each partner equally. The cost of building such a platform is not a one-time investment but one that will require an ongoing investment. Therefore, federal grant money needs to come with strings attached. States must be held accountable for creating a communications network—that is a dedicated channel shared channel capability for EMS, Fire, Law Enforcement, and Emergency Government—which will serve their entire state, allowing county and municipal governments full access. States redistributing federal grant money to county and municipal governments must ensure that the money is spent on compatible equipment and software to interface with the statewide platform.

The lack of common standards among venders continues to present difficulties of interconnection. If venders of equipment and software receive tax-supported dollars from states, counties, or municipal governments, they must be held accountable so that their products will create optimal technologies compatible with other venders' systems.

Being on the front line so to speak, troopers and other law enforcement officers throughout our nation rely on communications each and every day. Agencies must provide equipment that will allow our law enforcement officers to communicate with one another as well as the other disciplines of EMS, Fire, and Emergency Government.

As communication equipment users, we count on other law enforcement jurisdictions, EMS, and Fire several times a day during the regular course of duty. If we address the issue of interoperability at the basic level here, on the front lines, during these daily occurrences, we will have addressed a number of issues regarding localized emergency response: services involving multiple intra-jurisdictions; planned events including athletic events, conferences, and conventions; and regional incident management of natural and man-made disasters.

In closing, it is my assessment that currently federal tax-dollars are not being allocated, managed, or spent efficiently. Furthermore, there are no mechanisms in place to ensure accountability. Therefore, the lack of such coordination among our federal programs creates confusion and duplication of equipment and that end-users contend with on a daily basis.

I would be happy to answer any of your questions or to provide personal experiences related to my testimony.

Mr. REICHERT. Thank you, Trooper Perry.

The Chair now recognizes Mr. Bradley on behalf of the National Volunteer Fire Council.

STATEMENT OF TIM BRADLEY, SENIOR DEPUTY STATE FIRE MARSHAL, NORTH CAROLINA, ON BEHALF OF THE NATIONAL VOLUNTEER FIRE COUNCIL

Mr. BRADLEY. Thank you, Congressman Etheridge, for that fine introduction.

It is a pleasure to be here today.

Interoperability became a catch word after 9/11 and has increased since Hurricane Katrina, but it is important to remember that interoperability is not just about responding to hurricanes or terrorist attacks; it is being prepared to handle any kind of event that occurs.

It is also not about technology alone. It is about enhancing communications. That is the ultimate goal.

It can be reached only if the varying parties know not only what the other individuals said but what the individual is saying and what they mean.

Some of the necessities for enhancing coordination in addition to communication equipment is commonness in management terminology, common policies and procedures, standardized training and compatible equipment.

From a state perspective, North Carolina has been working on a system called VIPER, or Voice Interoperability Plan for Emergency Responders. It is a statewide system that will be available to all public agencies and is targeted to be complete in 2010.

The problem is that VIPER is not being used by most local agencies. Local government has simply not taken advantage of it due to cost. It is estimated that there are 75,000 individual radios in use by first responders in North Carolina, yet county to county, discipline to discipline, it is extremely fragmented. Few of those can talk to one another.

Interoperability communications was identified by the general assembly in 1995 as a problem, yet we still, agency to agency, cannot communicate well in our state.

From a federal perspective, the national preparedness goal for the Department of Homeland Security established strengthening interoperability communications as a primary goal and one of their seven national priorities.

Also on the federal level, following the creation of VIPER and which VIPER modeled very closely, the Office of Interoperability Communication and the Department of Justice's CommTech Program brought about and announced the first ever statement of requirements for public safety and interoperability.

SAFECOM released its first statements of requirements in 2004, and it defines future communication requirements for voice and data systems, as well as preparing the nation's 50,000 public safety agencies to develop a communication network. SAFECOM was designed to create interoperability solutions that are driven from the bottom up by the users.

From an accessed radio spectrum of 700 megahertz, Mr. Chairman, that you mentioned, first off, I would like to thank the members of this committee. You were leaders in getting that band released for first responders, and I would like to offer my personal appreciation.

But that band will be available for first responders in 2009. $1 billion in proceeds from the sale of radio-to-radio spectrum have been earmarked to assist public safety agencies in the use of this interoperable communications. This is just the tip of the iceberg in terms of the eventual cost for creating a truly national system of communications.

Cost is a concern for all fire departments, but particularly is acute for the volunteer fire departments like I served on. Many departments of this nature depend on private funding, private fundraising and donations. Fire departments that are always stretching their budgets just to survive are unlikely to remain operable with this kind of increase in technology simply because of the large amount of money required in expenditures.

So the challenges we face are that most departments have learned to deal with their problems, but the problems are going to be increased. For example, if one county puts in an 800 megahertz system, another county does not have it, ca not communicate with them and the issue of switching radio channels no longer exists from VHS to 800 megahertz.

From a recommendation standpoint, I would simply say that the federal government needs to get serious about implementing na-

tional communications interoperability. There has been many positive steps that have been mentioned, but if improving interoperability communications capabilities is really one of the seven national priorities critical to achieving DHS' goals, then there needs to be stronger federal coordination.

OIC is currently under the engineering and development section, which is under the Science and Technology Directorate in DHS. Interoperability really needs a higher profile within DHS and in the federal government, in general.

As I mentioned earlier in my print remarks, NTIA has been tasked with facilitating the transition to the radio spectrum in the 700 megahertz band of first responders and administering $1 billion currently set aside for that purpose. We think DHS would be the logical candidate to amend this program simply because of their prior work in dealing with first responders.

The federal government should continue to improve and encourage use of SAFECOM, not only seeing it as a recommendation but making it a requirement. We should consider establishing federal standards such as the App Code 25 SAFECOM to receive federal grants for communications. If we do not, counties, local government will continue to purchase equipment and still continue to be standalone agencies.

Last but not least, I would just like to say that in addition to providing this equipment and in addition to providing interoperability, one, we must continue to remember that state training agencies need funds to train first responders. You cannot be interoperable simply with equipment; you have to have the training as well.

Mr. Chairman, I will be happy to answer any questions after the panel members are through, and thank you for the opportunity to be here.

[The statement of Mr. Bradley follows:]

PREPARED STATEMENT OF TIM BRADLEY

WEDNESDAY, FEBRUARY 15, 2006

Introduction

Chairman Reichert, Ranking Member Pascrell, and distinguished members of the Subcommittee, my name is Tim Bradley, and I am Senior Deputy State Fire Marshal over the Office of State Fire Marshal in North Carolina, as well as volunteer Assistant Chief of the Mebane Fire Department and a member of the National Volunteer Fire Council, who I am representing here today. Thank you for the opportunity to provide you with my perspective on the issue of interoperability in communications.

In North Carolina the responsibilities of State Fire Marshal are with the Insurance Commissioner. The North Carolina Office of State Fire Marshal employs 106 individuals who coordinate building and fire codes; conduct building plan review; building code interpretations; as well as fire and rescue training; professional qualifications and certifications of first responders; and inspection of fire departments and fire incident reporting. We also work closely with our states emergency management office and serve as the coordinating agency for fire and rescue personnel and equipment during disasters. We work closely with 1289 fire departments, of which 967 are volunteer, 245 a combination of career and volunteer, and 77 career.

In my position I serve as State Fire Training Director and work closely with the National Fire Academy, International Fire Service Accreditation Congress, and other state training offices.

On a local level, I serve as volunteer Assistant Chief of a combination department that serves a community of 10,000 in a suburban and rural setting, and deals with two different County communication centers. I am a certified firefighter, Officer, In-

structor, Fire/Arson Investigator, Rescue Technician, and Life Safety Educator. I have been a volunteer firefighter for 32 years.

I also serve as an elected member of the City Council of our small community.

Interoperability Overview

Interoperability is a critical issue for the emergency services and affects metropolitan, urban, and rural settings. It has received varying levels of attention depending on which region of the country you live in. Interoperability became a catchword after 9/11, and again since Hurricane Katrina. However, interoperability isn't just about responding to terrorist attacks or natural disasters. Truly interoperable communications allow emergency responders to better coordinate their response to all types and all sizes of events.

Interoperability is also not just about technology and equipment. While my testimony focuses on communication, enhancing coordination is the ultimate goal and it can only be reached if the various parties responding to an event know not only what the others are saying, but what they mean. For example, in Indiana, a tanker is a truck full of water, while in California it is an airplane full of fire-retardant agents. Outside of interoperable communications, some of the necessities for enhancing coordination are:

—common incident management systems and terminology
—common policy and procedures
—standardized training
—compatible equipment

State and Local Perspective

North Carolina is working diligently on a state-wide communication system called VIPER, or Voice Interoperability Plan for Emergency Responders. This system will be available to all public agencies and is targeted to be completed by 2010. This does not mean all public agencies will all use it, and many will not due to costs of updating their existing equipment. Interoperable communications was identified in the General Assembly's Criminal Justice Information Network report of 1995 as a critical need for public safety agencies when responding to emergencies. It is estimated that there are over 75,000 individual radios in use in NC by first responders, yet county to county, discipline to discipline, it is extremely fragmented. I'm sure it mirrors the national trend.

It is estimated that State and local agencies in North Carolina, prior to the coordinated effort of VIPER, had already invested over $270 million in 800 MHZ technology, much of which would not be easily compatible with VIPER, even though VIPER is 800 MHZ. Hence the need for guidance and standardization. If you extrapolate that out on a national level, it would be astounding. If every state in the country had spent as much per capita as North Carolina on this technology, it would come out to a national bill of almost $10 billion.

Public safety officials in North Carolina should be able to communicate directly with other public safety officials without having to relay the message through a communications center. If put in place, VIPER interoperable communications would benefit all public safety agencies when dealing with daily emergency calls or large scale disasters. This will make fire, rescue, and law enforcement agencies better able to serve the citizens of North Carolina. The problem with the VIPER system is that most local governments are not taking advantage of it due to cost. It actually may become just another variable in a myriad of systems.

Federal Perspective

The overarching National Preparedness Goal for the Department of Homeland Security (DHS) is "to engage Federal, State, local, and tribal entities, their private and non-governmental partners, and the general public to achieve and sustain risk-based target levels of capability to prevent, protect against, respond to, and recover from major events in order to minimize the impact on lives, property, and the economy." When DHS established the goal in March 2005, one of the seven National Priorities identified as being critical to achieving success was strengthening interoperable communications capabilities.

SAFECOM

The creation of VIPER in North Carolina was followed very closely by the establishment of the SAFECOM program. SAFECOM is self-described as, ". . .a communications program within the Office for Interoperability and Compatibility (OIC) that provides research, development, testing and evaluation, guidance and assistance for local, tribal, state, and federal public safety agencies working to improve public safety response through more effective and efficient interoperable wireless communications."

OIC and the Department of Justice's CommTech program partnered to formulate the first ever Statement of Requirements (SoR) for public safety communications and interoperability. SAFECOM released the SoR in April 2004. The SoR provides the Nation's 50,000 public safety agencies with a document defining future communications requirements for both voice and data communications.

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 creating interoperability solutions that are driven from the bottom-up.

Access to Radio Spectrum in the 700 MHz Band

As I'm sure the Committee is aware, legislation was recently enacted that establishes February 17, 2009 as the date when parts of the 700 MHz band of radio spectrum, currently being used to transmit television signals, will be made available to first responders for communications. NVFC worked alongside other first responder groups for years to get a hard date set for the transition to take place. Many of our biggest supporters on this issue are members of this Committee and I'd like to take this opportunity to thank you for your leadership.

Now that we know when the spectrum will be available our focus turns to how it will be utilized. My understanding is that $1 billion in proceeds from future sales of radio spectrum have been earmarked to assist public safety agencies in acquiring, deploying, or training for the use of interoperable communications. This is just the tip of the iceberg when it comes to the eventual cost of creating a truly national system of communications interoperability, but it is an excellent start. While that funding is currently slated to be administered by the National Telecommunications and Information Administration (NTIA) at the Department of Commerce instead of DHS, I think that it is worth mentioning in any conversation about interoperable communications and because it demonstrates the tremendous cost implicit in transitioning thousands of fire departments' communications systems.

Cost is a concern for all fire departments, but it is particularly acute for thousands of volunteer departments. As noted in *A Needs Assessment of the U.S. Fire Service,* a 2002 study published by the National Fire Protection Association in conjunction with FEMA and the US Fire Administration, many volunteer departments depend on private fund raising to pay for operating expenses. Also, it is not uncommon for a volunteer department to rely on used equipment to save money. It is unlikely that fire departments that are already stretching their budgets just to remain operable would be able or inclined to invest a large amount of money to become interoperable.

Challenges

You cannot make fire departments nationwide interoperable until we make them operable, meaning having local communication systems that meet their needs. Most fire departments have learned to cope with their current communications problems internally, but when they respond outside their jurisdictions on mutual aid, either within the region or outside of it, multiple problems exist. If one county has strict use of 800 MHz systems, but does not use the low band and responds mutual aid to another county in the State that does, problems are encountered immediately.

Effective communication is based upon funding availability and system structure design within local areas. Many metro counties and systems seem to be ahead of the communication curve versus the rural areas and their systems. In fact, the advancement of technology has, in some cases, actually made the disparity between systems even greater. This is particularly disconcerting when you consider that rural areas, which are primarily protected by volunteer departments, contain the vast majority of our highway system, traveled by hundreds of millions each year.

Recommendations

The federal government needs to get serious about implementing national communications interoperability. There have been many positive steps in recent years, but if improving interoperable communications capabilities really is one of seven National Priorities critical to achieving the DHS' National Preparedness Goal there needs to be stronger federal coordination. OIC, which houses SAFECOM, is part of the Office of Systems Engineering and Development, which is under the Science and Technology Directorate at DHS. Interoperability needs a higher profile than this within DHS and in the federal government in general.

As I mentioned earlier, NTIA has been tasked with facilitating the transition of radio spectrum in the 700 MHz band to first responders and administering the $1 billion currently set aside for that purpose. DHS would be a logical candidate to administer this program because of its past work through SAFECOM and OIC and its experience dealing with first responders and first responder grants, which NTIA

lacks. NVFC would prefer to see responsibility for administering this program shifted to DHS. At the very least, NTIA should follow SAFECOM grant guidance.

The federal government should continue to promote the use of SAFECOM's Statement of Requirements for interoperability, mandating it to receive federal grants for communication equipment within states. Grants for communication equipment should be granted based on regional standardization, so that grant recipients purchasing communication equipments don't become stand alone agencies.

Nationally, we should consider the establishment of standards for communication interoperability instead of simply providing recommendations, so that when funds are expended for communication equipment by local government, it meets interoperability needs. Promotion of the National Incident Management System and the training and use requirements are a model of the attention given when programs are mandated rather than recommended. Do away with the ability of manufacturers to do their own thing in providing public communications and require APCO's Project 25 compliance when government agencies purchase equipment except, consistent with SAFECOM grant guidance, when a public safety agency cannot afford to do so.

We must provide State fire training agencies with funds and programs to train first responders, not only in communications, but in all areas of interoperability. Awareness often drives technology on the local level, and state training routinely gets left out when grants are awarded. Without a common training and standardization platform, any advances in technology or expenditures for equipment will be confusing, and counter productive.

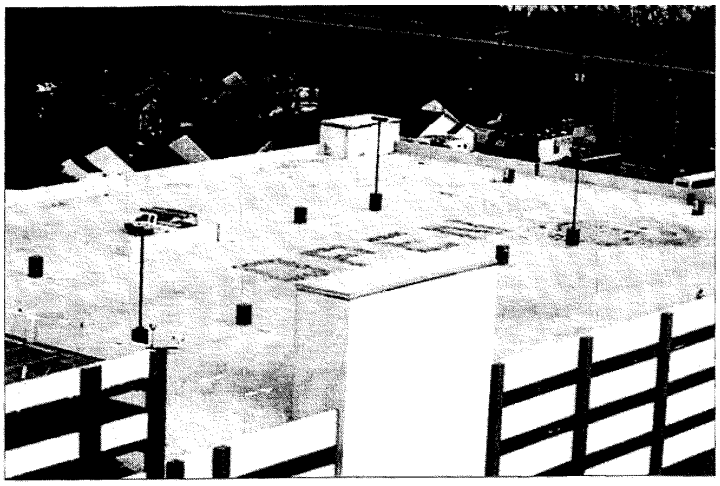
There must be a concerted effort to educate local and state government officials on the needs of first responders regarding interoperability. Local officials must be made aware of the impact of poor communications, not only during disasters, but during routine emergency operations. Interoperability will never occur with first responder awareness alone. Local government officials who control budgets must be convinced.

We need to reach out and explore how similar organizations accomplish command and control communications. These may include the military, UPS, Fed Ex or other agencies who manage large sums of information constantly. During disasters, FEMA must have a task group that immediately establishes communication mechanisms region wide to allow all incoming responders to be interoperable. This will be much easier if the local region has standardized protocols and equipment parameters.

Conclusion

I believe we have an opportunity to blend improvements in technology with needs of interoperability. The critical issue is that we must move rapidly to prevent that same technology from becoming another stumbling block.

It has been an honor and privilege to speak with you, I'll be happy to answer any questions you have.



Appendix A

Mr. REICHERT. Thank you, Mr. Bradley.
The Chair now recognizes Ms. Diane Linderman.

STATEMENT OF DIANE LINDERMAN, DIRECTOR-AT-LARGE, PUBLIC WORKS MANAGEMENT AND LEADERSHIP

Ms. LINDERMAN. Good morning, Chairman Reichert, Ranking Member Thompson and distinguished members of the panel.

My name is Diane Linderman, and I am the director of Urban Infrastructure and Development for VHB, Incorporated, in Richmond, Virginia, and formerly the Public Works director for the city of Richmond.

I am also director-at-large for leadership and management of the American Public Works Association, or APWA. I am here today on behalf of APWA's 27,000 members and our nearly 2,000 public agency members.

Public works officials are first responders. We work alongside police, fire and emergency service professionals to ensure that water is flowing through the fire hoses, traffic lights are operating and traffic is moving, barricades are up, debris is removed and the public is safe. We are often the last to leave the scene, as we manage the lengthy clean-up and restoration of any disaster site.

I appreciate the opportunity to speak today about interoperable communications and the indispensable role it plays in achieving an effective, coordinated emergency response. APWA has been, and will continue to be, an advocate for the development of policies which coordinate incident response across multidisciplinary agencies in a way that saves lives and restores communities' properties and critical lifelines.

My own experience as the director of Public Works in the city of Richmond when Hurricane Isabelle struck in September of 2003 demonstrates how vital interoperable communications is during an emergency. During the response and recovery, agencies, such as Public Works, Recreation and Parks, fire and law enforcement, were able to communicate. Regional system redundancies kept the system operating during and after the storm. The ability of fire and police to talk to the men and women clearing the streets of debris was necessary to effectively respond to calls for service, minimizing the impact on the health and safety of Richmond citizens.

The national discussion on interoperability has been centered on the need for people in different departments, different levels of government and mutual aid forces to be able to communicate.

Two issues stand out as fundamental. First, there continues to be a critical need for communication among responder groups to communicate effectively between other relief units and determine where resources are needed most. We cannot overemphasize the importance of having the ability to maintain uninterrupted communications. All of the compatible communications in the world will not help if the power and phone lines are down or backup power is not available.

In the aftermath of last year's catastrophic storms, stories of communication problems became an increasing subject of concern. For example, as response communications broke down during Hurricane Katrina, our understanding was that the most reliable communication backbone was e-mail, turning personal BlackBerry wireless devices into critical communication lifelines.

When an F4 tornado struck Missouri in 2003, the first problem encountered was the total loss of wireless and land-based phones when winds downed power cables, antennas and telecom lines. Using their personal radios, public works officials responded by relaying limited messages to City Hall until one of the main repeat-

ers was lost, forcing messages to be relayed through a nearby fire station radio instead.

As we develop solutions to these problems, greater emphasis should go towards making these systems more resilient during extreme conditions. To neglect this preparation is to invite further disaster in the midst of a catastrophe.

Reliable communications capabilities between all responders is critical to the efficiency and effectiveness of all response and recovery activities. In many cases, police have gone to 800 megahertz frequency radios, which they have received through federal grants, leaving public works with older high-band equipment. In such cases, public works can communicate through a dispatch center but cannot talk directly with police, fire or rescue personnel in the field.

In cases where public safety agencies are on digital and public works agencies are on analog, the ability to communicate is limited.

Additionally, the costs of obtaining digital radios is significant, and public works departments often do not have the resources to obtain them. Increased resources are needed to help local jurisdictions achieve interoperable communications.

The second fundamental issue of governance is non-technical. That is deciding who needs to communicate with whom, how and under what circumstances. Not every agency needs to have access to all information all of the time, but figuring out who does and when and obtaining agreement on the issue has been given very little consideration to this point.

Governance is an important tool to improve interoperability for public safety and emergency preparedness. That implies broadening the understanding of the barriers to effective interoperability at all levels, removing or overcoming the silo mentalities and turfism that exists among response agencies; demonstrating a willingness to collaborate with agencies with which emergency response is inevitable and recognizing that serving the needs of public safety is paramount.

Collaborative efforts like those that exist in the greater Richmond area through the Capital Region Communications Steering Committee can and do work. The Steering Committee was formed by a simple and short agreement signed by the three localities' executives in 1998. The Steering Committee sets policies and operational protocols while maintaining autonomy of operation by each locality. It is effective and a model to be emulated.

APWA recognizes the vital role interoperable communications plays in effective emergency response. It is more than simply a communications technology issue. It includes equipment as well as training, response team structure and operations. We see the need for increased funding for the equipment and training necessary to improve interoperable communications.

Mr. Chairman, thank you for the opportunity to testify this morning, and we look forward to being of assistance to you and your committee, and I will answer any questions later.

[The statement of Ms. Linderman follows:]

PREPARED STAEMENT OF DIANE LINDERMAN, PE

WEDNESDAY, FEBRUARY 15, 2006

Good morning, Chairman Reichert, Ranking Member Pascrell, and distinguished members of the panel. My name is Diane Linderman, and I am Director of Urban Infrastructure and Development for Vanasse Hangan Brustlin, Inc., in Richmond, VA and formerly Public Works Director for the City of Richmond, VA. I am also Director-at-Large for Public Works Leadership and Management of the American Public Works Association, or APWA.

I am here today on behalf of the 27,000 public works officials who are members of APWA including our nearly 2,000 public agency members. APWA is an organization dedicated to providing public works infrastructure and lifeline services to millions of people in rural and urban communities, both small and large.

I appreciate the opportunity to speak today about interoperable communications and the indispensable role it plays in achieving an effective, coordinated emergency response. APWA has been and will continue to be an advocate for the development of policies which coordinate incident response across multi-disciplinary agencies in a way that saves lives and restores communities, property and critical lifelines.

Let me take a moment to describe who public works officials are and what we do, and then I will go into more detail about the role APWA members play in preparation, response and recovery during catastrophes, and how interoperable communications is key to supporting these functions.

APWA's membership includes public works directors, city engineers, directors and senior managers of all areas of infrastructure, city managers, water and waste water treatment professionals among many others. Public works officials manage the very essence of our nation's communities: we manage the design, planning, and operation of critical infrastructures, including roads, bridges and water systems, and are on the front lines in the face of natural disasters, terrorist attacks and other public emergencies. We run the gamut of city services, with one overriding commonality: we are the nuts and bolts of local government. Public safety is our priority at all times.

Public works officials are first responders: we work alongside police, fire, and emergency service professionals to ensure that water is flowing through fire hoses; traffic lights are operating and traffic is moving; barricades are up; debris is removed; and the public is safe. Additionally, we are often the last to leave the scene as we manage the lengthy cleanup and restoration of any disaster site.

Public works officials know what it takes to make infrastructure less susceptible to damage from disasters as well as how to rebuild infrastructure after a disaster. We know how to get the roads and water mains in working order, how to restore power, how to rebuild or reinforce public buildings damaged by natural or man-made disaster, how to identify equipment needs, and how to assist other first responders in dealing with immediate threats.

Experience demonstrates how vital interoperable communications is during a catastrophe. During the terrorist attack on the Pentagon in September 2001, responders from local jurisdictions were able to communicate with each other but federal and military agencies could not communicate with the local responders nor could they communicate with each other due to the disparate communications systems and had no means to bridge the gap.

In another example, the I-95 Sniper attack of October 2002 in Hanover County, VA, immediately north of Henrico County and the Richmond metropolitan area, required a joint response by local and federal agencies. Hanover County uses an analog 800 MHz system which is incompatible with the Capital Region's digital, trunked 800 MHz system. Virginia State Police and federal responders' systems employ other frequencies, so interoperability was initially absent. Quick thinking on the part of Capital Region system managers solved the dilemma by gathering available portable radios from Henrico, Chesterfield and Richmond and reassigning them as needed to the Sniper Task Force while in the area.

With Hurricane Katrina, response communications were almost non existent. The few communications that were operational were not interoperable. One team of responders told us they had radio communications (base, mobile, and repeaters) but could not talk to many other responders due to lack of interoperability. This was true for many other responding teams. All had their own systems but were operating on various bands and frequencies. They were able to reprogram some systems to common frequencies but the ones that were operating on different bands caused a lot of communications problems. This not only leads to a response that is uncoordinated and inefficient but also created real safety issues to both the responders and to the public.

My own experience as Director of Public Works in the City of Richmond when Hurricane Isabel struck in September 2003 also demonstrates how vital interoperable communications is during an emergency. During the response and recovery, agencies such as public works, recreation and parks, fire and law enforcement were all able to communicate. Regional system redundancies kept the system operating during and after the storm. The ability of fire and police to talk to the men and women clearing the streets of debris was necessary to effectively respond to call for service, minimizing the impact on health and safety of Richmond's citizens.

The national discussion on interoperability has been centered on the need for people in different departments, different levels of government within a state, or mutual aid forces to be able to communicate. The focus of this point has been on the compatibility of technology and frequency management. Two issues stand out as fundamental. First, there continues to be a critical need for interoperable communications among responder groups to allow people to communicate effectively with other relief units, and determine where resources are needed most. We cannot over emphasize the importance of having the ability to maintain uninterrupted communications. All the compatible communications in the world will not help if the towers and phone lines are down or back-up power is not available.

Again, citing experience from Hurricane Katrina, the most reliable communication backbone was e-mail, turning personal BlackBerry wireless devices into a critical communications lifeline. Aside from email and the occasional satellite phone, there was no form of reliable communication between New Orleans and the outside world apart from BlackBerry devices. In many instances, hand written notes were used to communicate among responders. More attention is needed to understand how communications systems will hold up under extreme conditions. To neglect this preparation is to invite further disaster in the midst of a catastrophe.

The other fundamental issue related to communications interoperability is completely non-technological: that is, deciding who needs to communicate with whom, how (by voice, by data, and so forth) and under what circumstances. Solving the question of compatibility is relatively easy compared to establishing a set of protocols for an integrated federal, state and local communications interoperability matrix. Not every agency needs to have access to all information all the time, but figuring out who does and when, and obtaining agreement on this issue has been given very little attention to this point.

Reliable communication capability between all responders is critical to the efficiency and effectiveness of all response and recovery activities. Radio communication is a major issue and concern during emergencies and disasters. In many cases, police have gone to 800 MHz frequency radios which they have received through Department of Homeland Security grants. Public works is often left with older High Band. In such cases, public works can communicate through a dispatch center, but cannot talk directly with police, fire or rescue personnel in the field. Increased resources are needed to help local jurisdictions achieve interoperable communications. In cases where public safety agencies are on digital and public works agencies are on analog, the ability to communicate is limited. Additionally, the cost of obtaining digital radios is significant and public works departments often do not have the resources to obtain them.

As first responders, we urge that funding for radio communications grants be targeted specifically to public works departments. Currently, because of the insufficient funding towards improving interoperable communications, states in some cases are not pushing adequate funds down to local jurisdictions because of the cost of implementing their systems. In Illinois, the state's STARCOM radio system is costing millions to implement and will provide every community with one radio. However, additional radios will cost local agencies between $6,000 and $7,000 each. One community in Illinois just received a new VHF 150 MHz channel for a city-wide communications band, but public works will have to re-radio their fleet to accomplish that, at a cost of about $100,000. With local budgets oversubscribed, many communities cannot afford these kinds of costs.

Interoperable capability also needs to include strengthening our existing phone/cell/radio systems. In Missouri where an F4 tornado struck in 2003, the first problem was the loss of all cell phone and land lines when the wind disrupted the power and phone lines and damaged antennas. Public Works was able somewhat to relay messages to city hall through their radios. However, one of the main repeaters had been lost, so the messages had to be relayed through a nearby fire station radio. The public works department had assistance from other area cities and counties through face-to-face communications only, because the radios were not on the same frequencies.

In addition to resources, governance is an important tool to improve interoperability for public safety and emergency preparedness. That implies broadening the

understanding of the barriers to effective interoperability at all levels; removing or overcoming the silo mentalities and 'turfism' that exists among response agencies; demonstrating a willingness to collaborate with agencies with which emergency response is inevitable; and recognizing that serving the needs of public safety is paramount. Joint training and disaster reaction drills with team partners in law enforcement, fire and related agencies is critically important. Good working relationships are key to establishing who is in charge and who is responsible for what.

Collaborative efforts like those that exist in the greater Richmond area through the Capital Region Communications Steering Committee (CRCSC) can and do work. To address the months of wrangling between neighboring jurisdictions who in the past often failed to reach desired mutually beneficial objectives, the CRCSC was formed by a simple and short MOU signed by the three localities' executives in 1998. The CRCSC sets policies and operational protocols while maintaining autonomy of operation by each locality. It is effective and, in our opinion, a model to be emulated.

In addition, the Department of Homeland Security's Science and Technology Directorate's Office for Interoperability and Compatibility has the SAFECOM Program. It is a communications program that provides research, development, testing and evaluation, guidance and assistance for local, tribal, state, and federal public safety agencies. Through more effective and efficient interoperable wireless communications, SAFECOM is working to improve the public safety response in a meaningful way.

APWA has an Emergency Management Technical Committee within our organization that has consistently supported, provided comments for and helped to implement HSPD–8, the National Response Plan (NRP) and the National Incident Management System (NIMS). We continue to support an emphasis on cross-discipline communication, interoperable communications and training for our members, public officials and all first responder groups.

Public works personnel have been available to interoperable communications groups over the past four years. As we have in the past, we are again serving on the President's HSPD–8 working group, with a goal to "establish policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies."

APWA recognizes the vital role interoperable communications plays in effective emergency response. Interoperable communications is more than simply a communications technology issue. It includes equipment as well as training, response team structure and operations. As first responders, we see the need for increased funding for the equipment and training necessary to improve interoperable communications so that we can be better prepared for the challenges we will all face in the future. Through cooperation, training and additional resources, we believe that we can achieve better response and recovery capabilities for the communities we serve.

Mr. Chairman, thank you again for the opportunity to testify this morning. We look forward to being of assistance to you and the subcommittee. I will be happy to answer any questions you may have.

Mr. REICHERT. Thank you, Ms. Linderman.

The Chair now recognizes Mr. Moroney.

STATEMENT OF WILLIAM R. MORONEY, PRESIDENT AND CHIEF EXECUTIVE OFFICER, UNITED TELECOM COUNCIL

Mr. MORONEY. Thank you, Mr. Chairman, members of the subcommittee. My name is Bill Moroney, and it has been my honor for the last 8 years to serve as the president and CEO of the United Telecom Council.

For nearly 60 years, UTC has been the voice of electric, gas and water utilities on telecommunications matters. UTC's several hundred members range from large investor-owned utilities to municipalities, to coops operating in big cities, smaller towns and rural areas throughout the country.

These utilities own, maintain and operate private mission-critical communications systems, including ultra-reliable two-way radio networks. And these systems are vital to their safe and efficient operation. I appreciate the opportunity to appear before you today

and discuss some issues of vital concern to all emergency responders.

I would like to make three important points today. One, power and water utilities require reliable interoperable communications to provide services considered necessary for normal life.

Two, effective and interoperable communications are needed, both among utilities responding to emergencies and between them and public responders, something we do not generally have today.

And, three, government oversight of emergency preparedness and interoperability that mandates inclusion of the entire emergency response community in policy and planning.

The job of an electronic company lineman is nearly always listed among the 10 most dangerous jobs in the nation. Communications networks, especially our private radio systems, are considered safety equipment to utility crews just as they are to police officers and firefighters. Safe operations and rapid restoration of service in emergencies are not possible with these systems.

It is understood that police and fire personnel are among the first responders to an emergency, but utility workers, who also immediately race to disaster-stricken areas, are all too often overlooked as vital to any emergency response planning, even though the most important step back to normal life following any disaster is the restoration of electric power and supplies of safe drinking water to homes and businesses.

We use the term, "emergency responders," to encompass a broader community than traditional first responders. We recognize a distinct difference between police and firefighters, traditional public safety and the rest of the emergency response community.

We use the term to include all of us who are on the ground responding within minutes and hours to disasters of all kinds.

Utilities support emergency response by building highly robust communications systems. Simply put, these systems are designed to keep working when the power is out. That is a fact that makes us excellent partners as the nation looks for interoperability solutions.

Recently, the communications systems—our land mobile radio systems, microwave and fiber optic networks—owned by the most Gulf coast utilities, large and small, continued to function or were back up within hours during and after Hurricanes Katrina, Rita and Wilma. This is in contrast to nearly all other communications networks in the area. This is just one finding from a recent UTC research study that has been provided to the subcommittee and attached to part of my statement.

Tens of thousands of utility field crews from around the United States and Canada responded to the hurricane-stricken areas in both 2004 and 2005. They do the same after ice storms in the North or other disasters, and just this week crews from other utilities could be seen around the Washington area helping restore power after this weekend's snowstorm.

While local utilities generally get excellent performance from their communications systems, one of the major problems for coordinating such large-scale restoration efforts is the fact that utility communications systems themselves are not often interoperable with other utility systems. Our members operate on several dif-

ferent frequency bands, using different technologies like everybody else here today.

Therefore, our need for interoperability emergency is twofold: We need communications among crews from different utilities, and we need much better coordination between utilities and the traditional public safety community.

Unlike public safety, critical infrastructure industries have not dedicated spectrum for our use. The spectrum we use is shared with incompatible users like pizza delivery companies and taxi companies and is becoming increasingly congested and is subject to harmful interference.

So how does the federal government help us get to real interoperability? Utilities should be designated as an emergency responders along with everybody else who is racing toward the problem and should be included in the preparedness and response planning.

And with a small nationwide spectrum allocation of 6 to 10 megahertz, utilities could build a next-generation voice and data network that would not only make utilities more efficient during disaster recovery but could also be made available to all emergency responders as needed. More details on this proposal are attached to my written statement as well. And we believe that congressional leadership is needed here.

Utilities build the most robust communications infrastructure in our country. This combined with our strong habit of emergency planning and response operations we believe makes us excellent partners in the drive toward interoperability.

UTC and its hundreds of members stand ready to help in any national efforts to make the United States both more prepared for a disaster and more equipped to recover from it quickly, but, Mr. Chairman, we need your help.

Thank you very much for the opportunity to speak with you. I will be glad to answer your questions later.

[The statement of Mr. Moroney follows:]

PREPARED STATEMENT OF WILLIAM R. MORONEY

WEDNESDAY, FEBRUARY 15, 2006

Mr. Chairman and honorable members of the Subcommittee:

I am William R. Moroney, President and Chief Executive Officer of the United Telecom Council (UTC). I thank you for the opportunity to appear before you today to discuss issues of vital concern to all emergency responders.

For nearly 60 years, UTC has been the voice of electrical, gas and water utilities in matters relating to their voice and data telecommunications. UTC's several hundred critical infrastructure members range in size from multi-state organizations such as National Grid and Exelon, to municipally owned utilities and co-ops operating in cities, towns and rural areas throughout the country. All of these companies own, maintain and operate private, mission-critical communications systems. Most importantly for purposes of this hearing, these include two-way land mobile radio systems on which we all rely for both routine and emergency communications.

Critical Infrastructure Communications Affect Homeland Security

All critical infrastructure industries are becoming increasingly dependent on information management and private internal communications systems to control and maintain their operations. A 2002 study by the National Telecommunications and Information Administration (NTIA), entitled, "Current and Future Use of Spectrum by the Energy, Water and Railroad Industries," makes very clear the extent of this

dependency to meet essential operational, management and control functions.[1] Communications systems, especially radio systems, are considered safety equipment just as they are by public safety personnel. Safe operations and rapid restoration in emergencies are not possible without these systems.

All parties concerned with homeland security agree that one of the most important considerations is the availability of reliable, interoperable communications for "emergency responders," a term we use to encompass a broader community than traditional first responders. It's meant to include all those who are on the ground responding within hours to disasters of all kinds. Another fact brought to attention by recent events, especially the disastrous hurricanes of the past two years, is that the most important step back to "normalcy" is the restoration of electric power and a supply of safe drinking water to homes and businesses.

In this regard, there are three important issues which need to be addressed: 1) The critical players that require such communications include not only the first responders from the public safety community, but also the critical infrastructure enterprises such as power and water utilities that provide services considered necessary for normal life; 2) We must ensure effective and interoperable communications both among critical infrastructure entities responding to emergencies, and between them and public safety responders; and 3) Government oversight of emergency preparedness and interoperability must mandate inclusion of the entire emergency response community in federal policy and planning to overcome local biases and coordinate what are now only piecemeal efforts.

Emergency Responder Communications

It is understood that the local and state police and fire personnel are among the first responders to an emergency, as well as emergency medical personnel. But critical infrastructure employees—the utility workers who immediately head to disaster-stricken areas and get to work—are often overlooked as vital to any emergency response. Along with protecting life, the first order of business following a manmade or natural disaster is the restoration of essential public services, including water (to fight fires and ensure clean and safe supplies), gas and electricity (to restore heat, light, computer-based networks of all kinds, commercial communications, and more). These are the first services that must be brought back on line, so these workers are among the first personnel on the scene.

The job of an electric lineman is nearly always listed among the ten most dangerous in the nation—and reliable communications is key to safety, especially in the chaos that follows a disaster. One element of reliability for critical infrastructure industries, beyond that for traditional public safety: our radios must work, wherever our crews go, when the power is out. During any kind of manmade or natural disaster, you will see police, fire, utility and other emergency personnel on the scene at the same time. **Any discussion of emergency interoperability must include critical infrastructure industries such as electric, gas and water utilities if the United States is to have an effective system.**

Some examples: as soon as the magnitude of the 9/11 disaster became apparent, more than 1900 Consolidated Edison emergency workers were dispatched to Ground Zero to assist critical service restoration efforts and provide emergency communications capabilities to others on the scene. ConEd's two-way land mobile radio system was among the only communications available and was widely used during the first few hours following the collapse of the Twin Towers. More recently, the communications systems—land mobile, microwave and fiber—of Gulf Coast utility companies, large and small, continued to function or were back up within hours during and after hurricanes Katrina, Rita and Wilma, in contrast to nearly all other communications networks. This performance is documented in UTC's November 2005 study, *Hurricanes of 2005: Performance of Gulf Coast Critical Infrastructure Communications Networks.* The findings of the study, as outlined in its Executive Summary, are included with this statement as Attachment B.[2] Among them is the highlighted need for better interoperability to get the work done safely and as fast as possible.

Moreover, utility emergency response is usually a nationwide, and even international, response. Tens of thousands of field crews from around the U.S. and Canada responded to hurricane-stricken areas in both 2004 and 2005; they do the same after ice storms in the North or any other disaster. This week, crews from other utilities could be seen around the Washington area helping to restore power after this

---

[1] A copy of the Executive Summary of the NTIA Study is included as Attachment A to this document. The full study can be found at *http://www.ntia.doc.gov/osmhome/reports/sp0149/sp0149.pdf.*

[2] The full text of the study will be provided to the Subcommittee as supplemental material, or may be found at *http://www.utc.org*

weekend's snowstorm. While local utilities generally get excellent performance from their communications systems, one of the major problems for coordinating such large-scale efforts is the fact that utility communications themselves are not interoperable. Our entities operate on several different land mobile frequency bands, using different technologies. *Therefore, critical infrastructure's need for interoperability in emergency response is two-fold: we need communications among crews from different utilities, and we need much better coordination between utilities and local public safety agencies to facilitate restoration.*

Local Efforts Toward Interoperability

Congress recognized the importance of our systems in 1997, when you included utilities, pipelines and other critical infrastructure among "public safety radio services:" those private systems that provide support to such vital systems that entities operating them should have access to spectrum without obtaining it via auction. Since then, critical infrastructure has not sought access to existing public safety spectrum. However, the FCC has not made an allocation to non-public safety private wireless since 1985, and critical infrastructure industries, unlike Public Safety, have no dedicated spectrum for their use. Therefore, UTC and its members have looked for opportunities to bolster interoperability among all emergency responders by other means, while continuing to seek a dedicated spectrum allocation. The most effective means on a local basis has been through shared radio systems shared among multiple agencies including utilities and traditional public safety, and there are dozens of these throughout the country.[3] Many of them have been built by utilities, because we often can get the system funded and into operation faster than public safety agencies. And—we build our systems so they work when the power is out.

Just a few examples of shared systems: Gainesville, Florida, where Gainesville Regional Utilities has built and maintains a non-profit, shared 800 MHz system. Local public safety agencies use this system as low-cost subscribers. There are many municipalities, as throughout the Philadelphia metro area, where local utilities and public safety agencies share a common radio system owned by the local government.

In Mississippi, Alabama, Georgia and the Florida Gulf Coast, Southern Company has built a commercial 800 MHz system to utility standards, making it attractive to thousands of public safety users, as well. The Southern system was among the utility systems that remained operational post-Katrina, when all other cellular systems were down. A system like Southern's is the only form of commercial system appropriate for mission-critical communications, since utilities must have complete coverage of their service territories, as well as guaranteed reliability at all times. No consumer-oriented commercial wireless provider can afford to offer service to this standard, nor do commercial systems continue to function during power outages of any duration.[4] Utility communications must function ultra-reliably, and never more so than when the power is out. Since commercial communications networks cannot meet this standard, they generally are not relied upon for emergency or mission-critical communications.

The shared systems outlined above are only local or company-specific attempts to solve interoperability problems, and the United States needs a nationwide solution so that all emergency responders can communicate with each other. We offer our expertise to help reach this vital goal.

Critical Infrastructure Could Build an Interoperable Network

Unlike traditional public safety, the critical infrastructure industries have no designated spectrum for their own use, and we suffer from increasing congestion and interference on the bands we share with millions of other non-public safety private wireless users. We have requested a small, exclusive allocation of six to ten megahertz on a band below 1 GHz, on which we propose to construct a nationwide system. This system would be interoperable among the many critical infrastructure entities that always respond to regional emergencies, and would be made available to traditional public safety, federal agencies and others through additional equipment, or as part of a network of networks (*see* Attachment C, below).

---

[3] While most shared systems include a municipal utility, UTC is aware of a pending statewide system in Missouri that is designed to include various public safety agencies and investor-owned utilities. Such a system, if encouraged by state leadership, could become a model of cooperation for other areas.

[4] The Subcommittee should take notice that programs promoting commercial wireless providers for Wireless Priority Access Service are completely useless to critical infrastructure. Even if not overloaded with traffic during a disaster, whether manmade or natural, cellsites do not have long-term backup power. A system that simply doesn't work during power outages—regardless of our low priority to start—is useless to critical service restoration personnel and should be considered useless for public safety personnel, as well.

While it is understood that spectrum is a scarce resource, homeland security initiatives should consider an exclusive allocation of spectrum to critical infrastructure for the establishment of a nationwide emergency communications network. This would achieve three objectives: 1) economies of scale would drive down the cost of equipment; 2) efficient spectrum use would dictate the use of this spectrum on a day-to-day basis for critical infrastructure operations support, while entities would be responsible for maintaining the emergency network; and 3) emergency response capability would be served by all response agencies having immediate access to fully operational communications equipment, priority access and a fully interoperable network when the need arose.

Federal Coordination is Necessary

One of the questions posed for this hearing concerned the appropriate role of the Federal government in interoperability efforts. To begin with, UTC does not believe that this government is prepared to, or should, fund a stand-alone emergency system for just a portion of the emergency response community. Not only would this be ruinously expensive, it would be an extremely inefficient use of scarce spectrum, would duplicate existing systems and would not appreciably help emergency response as it occurs in real life. Instead, Federal coordination is needed to ensure that all segments of the emergency response community are included in planning efforts, whether national, state or regional, and to encourage coordination among national representatives to develop policies and procedures that will help entities work together. For example, non-local utility crews often are stopped by law enforcement from getting into damaged areas to restore power; a simple, standard procedure could eliminate this problem. **The Federal government should designate critical infrastructure industries such as utilities as "emergency responders," and mandate their inclusion in preparedness and response planning.** Congressional leadership also is needed to establish the spectrum allocation outlined above—while UTC has great respect for the Federal Communications Commission and its personnel, the agency's focus on commercial communications services has made it less than well-equipped to understand or act on the needs of non-commercial licensees.

UTC and its hundreds of members stand ready to help in national efforts to make the United States both more prepared for disaster, and more equipped to recover from it quickly. Critical infrastructure entities build the most robust communications infrastructure found in the U.S., as proven by its performance, and our strong habit of emergency planning and operations makes us excellent partners in the drive toward efficient emergency response and recovery. We urge you to include us in interoperability development and implementation.

ATTACHMENT B

Hurricanes of 2005:

Performance of Gulf Coast Critical

Infrastructure Communications Networks

November 2005

A Research Study by the United Telecom Council

1.0 Executive Summary

The hurricane season of 2005 resulted in immense damage and tragic loss of life to Florida and the Gulf Coast of the United States. Storms Katrina, Rita and Wilma also pointed out the weaknesses in many of our critical infrastructures, including telecommunications networks, some of which are still recovering months later. **However, in sharp contrast to many commercial wireless, landline telephone and other telecommunications networks, the private, internal networks (radio, microwave and fiber) of electric, gas and water utilities for the most part continued to function throughout and immediately after the storms.** In some cases, it was utility communications networks that provided the only reliable communications among emergency responders and other officials during the first few days after the storms.

The reliable performance of these internal systems was neither unexpected nor unusual; utility communications systems are constructed specifically to withstand major disasters. The United Telecom Council (UTC), the international trade association representing the telecommunications interests of critical infrastructure indus-

tries,[5] has conducted informal polling of its members after such emergencies as a major Northeast ice storm in 1998; the huge electric blackout of August 2003; and the hurricanes of 2004, with similar results.

However, given the magnitude of this year's disasters and resulting national discussions concerning the survivability of communications networks, UTC felt it imperative to undertake a formal survey of Gulf Coast electric, gas and water utilities of all sizes, to generate data that would quantify our anecdotal information.

Overall findings:

- All by one of impacted CII entities responding reported that their communications networks generally survived the hurricanes and continued to operate well throughout restoration efforts (the single exception was a utility that relied on commercial wireless service;
- Private land mobile radio (LMR) networks provided critical communications among crews; however, the huge number of responding entities from around the country taxed capacity or could not operate on local systems, pointing up the need for CII interoperability;
- Utility fiber and microwave systems survived and generally continued to function; however, this was due in part to built-in redundancies, robustness and recovery mechanisms that would be cost-prohibitive for a for-profit network designed to serve the general public. Therefore, CII entities will continue to require private networks to meet mission-critical needs for the foreseeable future, along with the ability to expand them as needed to meet system growth requirements.
- Unfortunately, there was little or no formal coordination with state or local agencies or public safety organizations during or after the storms. Given the opportunities for improved response communications offered by robust CII systems, and the presence of CII personnel "on the ground" in nearly every disaster scenario, this lack emphasizes that CII MUST be included in emergency response planning at the Federal level.
- We believe these findings should be of significant importance to Congress and to Federal agencies charged with communications-related Homeland Security responsibilities, such as the Federal Communications Commission and the Department of Homeland Security. UTC and its members look forward to discussing these findings and their implications with policymakers and others.

[Note: the full text of the report is being provided to the Subcommittee as supplemental material]

ATTACHMENT C

U.S. Emergency Wireless Network—

A Responder Build-out Proposal

All parties concerned with homeland security agree: one of the primary needs in any emergency situation is reliable communications, interoperable among all responding entities. Due to its long-standing regulatory framework and division of jurisdiction over radio-frequency (RF) spectrum, the United States currently has no such capability. Whether manmade or natural, emergencies leave traditional public safety agencies, utilities and other responding critical infrastructure entities, and relevant federal agencies unable to communicate effectively either among themselves or with other responders, at the time it is needed most. This serious gap in capability, witnessed after the September 11, 2001 terrorist attacks and natural disasters such as the hurricane season of 2004 and 2005's Hurricane Katrina, must be addressed.

The United Telecom Council (UTC), the voice of critical infrastructure (CI) telecommunications since 1948, is among the many parties seeking a solution to this difficult problem. In addition, UTC is increasingly concerned that **critical infrastructure industries have no spectrum dedicated for their exclusive use on any frequency band,** as noted in the 2002 National Telecommunications and Information Administration (Commerce) study of current and future spectrum use by the energy, water and railroad industries. CI wireless voice systems currently operate in bands shared with many incompatible uses. Mission-critical telemetry and

[5] UTC's membership consists primarily of publicly-held, municipal and cooperative electric, gas and water utilities and gas pipelines, and Federal power authorities. Through affiliated association members, UTC reaches out to other Critical Infrastructure

Industries (CII) as defined by the FCC in Section 90.7 of its Rules (47 CFR § 90.7), including petroleum and oil pipeline companies and railroads.

SCADA systems are often found on bands where they have only secondary status and may be required to cease operations, and all CI communications face increasing congestion and harmful interference. Moreover, different utilities do not use the same spectrum for the same operations because of varying frequency availability across the Nation, thus hampering cooperative efforts in times of emergency. However, in spite of these difficulties, utility telecommunications systems—because they are built to support restoration, preserve personnel safety and underlie the reliability of electric, gas and water service—generally prove to be the most robust in times of emergency.

Proposal

UTC proposes to solve all these problems simultaneously, by a means we believe would: 1) cost less; 2) use spectrum more efficiently; and 3) meet the needs of emergency responders more closely than other proposals. Utilities and other CI entities traditionally work closely with traditional public safety agencies: they respond to the same emergencies, but utilities generally have more emergency-reliable wireless communications due to construction methods. In fact, CI entities increasingly help to build traditional public safety radio systems and/or share frequencies with public safety agencies. ***Congress and the FCC recognized the close working relationships among these entities when they re-classified utilities, pipelines and other CI entities as "public safety radio services" along with more traditional public safety organizations such as police and fire departments.***

To promote faster, more reliable and interoperable emergency response, as well as to meet the urgent communications needs of CI entities for the next decade or more, UTC proposes an innovative use of scarce RF spectrum:

To meet everyday needs for reliable wireless voice and data communications, UTC urges a small CI nationwide spectrum allocation of 6-10 MHz in a frequency band below 1 GHz;

CI entities would construct infrastructure nationwide, implementing an integrated voice and data technology platform providing an interoperable communications system. Utilities and other CI entities would migrate to this system over time (an estimated 7–10 years, based on equipment life cycles). Migration and build-out could be accomplished more quickly with partial Federal funding. Additional, fully operational equipment would be kept on hand by local CI entities using the system. In emergency situations, all traditional public safety, federal and other agencies would have immediate access to this equipment. A system of emergency priority access to frequencies also would be implemented to ensure reliable access for emergency responders.

An alternative interoperable system would consist of a "network of networks," in which CI entities, traditional public safety agencies and other emergency responders would designate existing frequencies to an interoperable network during emergencies, all entities retaining control over their existing networks. With nationwide designated spectrum, CI entities could build and maintain the technology platform necessary to make this system possible.

Either method of interoperability would ensure that scarce spectrum resources are used efficiently, while providing the widespread access to joint communications needed urgently to meet U.S. emergency response needs. Given the long-time expertise in infrastructure build-out by CI entities, coupled with their deep understanding of emergency communications needs, UTC believes this proposal would provide for the type of nationwide emergency communications system most needed, built by the best-qualified entities.

UTC is anxious to discuss its efforts in this direction and means by which this proposal may be implemented, and looks forward to working with your office to develop it further.

Mr. REICHERT. Thank you, Mr. Moroney.

Dr. William Pinsky is now recognized.

STATEMENT OF WILLIAM PINSKY, EXECUTIVE VICE PRESIDENT AND CHIEF ACADEMIC OFFICER, OCHSNER CLINIC FOUNDATION, NEW ORLEANS, LOUISIANA

Mr. PINSKY. Good morning, Mr. Chairman, distinguished committee members.

As Representative Jindal introduced me, I am Dr. William Pinsky, a pediatric cardiologist and the executive vice president

and chief academic officer of the Ochsner Clinic Foundation in New Orleans, Louisiana.

On behalf of the American Hospital Association's 4,800 hospitals, health systems and other health care organization members and our 33,000 individual members, I appreciate the opportunity to appear before you today.

Ochsner, which has 478 acute-care beds in the main hospitals, and 24 clinics throughout the New Orleans area and 4 clinics and a hospital in Baton Rouge, is not a not-for-profit comprehensive integrated health care system, the largest non-governmental employer in Louisiana and a center of excellence in research, patient care and education.

Throughout Katrina's onslaught and its devastating aftermath, we remained open, caring for patients.

This morning, I would like to tell you how we prepared for the storm, what we did to ensure our communications systems worked, how we kept our doors open and answer questions you may have about our experience.

Hospitals routinely plan and train to deal with disasters, both natural and manmade. Our plan, revised after every disaster or near-miss event, was updated less than 3 months before Hurricane Katrina struck.

On Friday, August 27, when we were notified that the storm would likely hit the area, we immediately initiated the first phase of our plan: Notifying essential personnel and securing previously stockpiled supplies. Staff began discharging appropriate patients and moving those unable to leave the facility into areas thought to be the most secure. We then settled in and waited.

We sustained structural damage, but overall the news was positive. Our emergency generators functioned, our internal communications system and internet were fully operable. We had adequate supplies, we believed we would ride out the next few days until help arrived.

It was not easy, but we faired well in the beginning. On day 2, an emergency generator failed, forcing us to go without air conditioning. As a result, we shut down our internet server to prevent heat damage, losing our electronic medical records system. Luckily, we were able to repair the generator the next day and restore full operations.

We had made extensive plans for securing and relieving essential personnel, going to great lengths to keep staff apprised of the situation, setting up a telephone tree as well as a dedicated Web page with information. And we found ourselves in some difficulty in reaching our relief staff.

We were eventually able to locate the staff and brought them to Baton Rouge and then conveyed them into New Orleans by bus convoy. Those same convoys were our lifeline to supplies as well, enabling us to continue functioning.

With the situation in our main facility in hand, we sought to offer our assistance to others. However, we had great difficulty contacting the proper authorities, finding it hard to even locate state and federal officials to offer our assistance.

According to our regional emergency plan, we were to report to the Jefferson Parish Office of Emergency Preparedness. When our

attempts to reach them failed, we explored other channels. Eventually, we were able to contact the Orleans Parish office. From them we learned of their communication difficulties with evacuating downtown hospitals. It was virtually impossible to coordinate air evacuations due to the various agencies involved, both military and civilian, and the lack of ability to communicate.

Police communications systems were ineffective because of infrastructure damage and the volume they were trying to handle. The National Guard system was able to facilitate communications among Guard units but had difficulty communicating with local authorities.

Communication improved on day 4 when the United States Public Health Service arrived. They were able to facilitate requests through the previously blocked channels. However, they did not have many of the assets we required.

Prior to their arrival, we were not able to alert authorities that we were functioning and could receive patients. We even went as far as using large trash bags on the garage of our roof to spell out the word, "open," to attract the attention of helicopters overhead.

In light of the events, we are revising our disaster policy, and I am very interested in improving our ability to communicate with authorities and others in future emergencies.

In conclusion, we survived Hurricane Katrina as well as could be hoped for because of the communication difficulties with the outside world, we became self-sufficient, securing our own methods of sustaining our facility. We were able to do this primarily because our facility in Baton Rouge could be used as an off-site command post and because our own communications system remained operational through built-in redundancy. However, we could have done much more to assist the authorities and the local community if a fully interoperable communications system had been in place.

Communication with local, state and federal authorities is crucial for ensuring that hospitals can fulfill their mission during disasters.

We look forward to working with the committee and the staff toward a shared goal of improving the disaster preparedness for America's hospitals and communities.

Thank you.

[The statement of Mr. Pinsky follows:]

PREPARED STATEMENT OF WILLIAM W. PINSKY, M.D.

WEDNESDAY, FEBRUARY 15, 1006

Good morning, Mr. Chairman. I am William W. Pinsky, M.D., executive vice president and chief academic officer of Ochsner Clinic Foundation (OCF), in New Orleans, La. On behalf of the American Hospital Association's 4,800 hospitals, health systems and other health care organization members, and our 33,000 individual members, I appreciate the opportunity to speak to you and your colleagues about the importance of interoperable communications during a disaster.

For nearly 60 years, OCF has cared for residents in the greater New Orleans and Baton Rouge communities. Our main campus, including the 478 acute-care bed hospital and clinic, is located in Jefferson Parish, less than a mile from the Orleans Parish line and only a 15 minute drive to downtown New Orleans. In addition, we have 24 clinics throughout the New Orleans area and a sub-acute nursing facility/inpatient psychiatry/inpatient rehabilitation hospital two miles from our main campus. In Baton Rouge, we have three clinics, 70 physicians and 50 percent ownership of an acute care hospital. Recognized as a center for excellence in research, patient

care and education, OCF is a not-for-profit, comprehensive, integrated health care system, and the largest non-governmental employer in Louisiana. With more than 7,400 employees—including more than 600 physicians in nearly 70 medical specialties—OCF is also one of the largest non-university-based physician-training centers in the country, annually hosting over 350 residents and fellows, 450 medical students and 400 allied health students.

When Hurricane Katrina hit the Gulf Coast, no one could have truly imagined the intense devastation it would leave in its wake. The wind and the rain wreaked havoc across Alabama, Mississippi and Louisiana. Knowing that the storm was headed their way, hospitals began sending home patients deemed well enough to be discharged. Those in critical condition or requiring special assistance, such as ventilator-assisted breathing, remained in the hospital. When hospital staff emergency teams arrived for work during the weekend before the storm hit, they expected it might be only a few days before they were able to return home. However, when the levees in New Orleans broke, the situation changed dramatically. We, and our colleagues in the New Orleans metropolitan area, faced a dire situation beyond our imagination.

Throughout the onslaught of Hurricane Katrina, and during its devastating aftermath, OCF remained open, caring for patients. This morning, I'd like to tell you how my hospital prepared for the storm; what our facilities did to ensure our communication systems worked and our doors remained open to provide critical health care services to our community; and answer any questions you and your colleagues might have about our experience.

Planning for Disaster

Hospitals routinely plan and train to deal with disaster, whether it's the derailment of a train carrying hazardous substances, a multiple-vehicle accident on a nearby interstate, a plane crash, or a natural disaster such as a hurricane or earthquake. As hospitals plan for disasters and the prospect of going without public services such as electricity and water, we prepare to be on our own for at least 72 hours, in the event it takes that long for assistance to arrive from the state or federal government. Our plan, which we revise after every disaster or "near-miss" event, had been revised most recently on June 1, 2005, less than three months before Hurricane Katrina struck.

On Friday, August 27, our entire executive leadership team had assembled in New Orleans for the first day of a two-day leadership retreat. Late in the afternoon, we were notified that the storm had turned to the West and likely would strike the area. We immediately initiated the first phase of our disaster plan, which included notifying essential personnel and securing previously stockpiled supplies.

Under the most recent disaster plan, two teams of essential personnel, Teams A and B, were created to ensure continuity of care and relief for employees on duty at the time disaster strikes. Each team was to include staff members from all departments, e.g. security, housekeeping, dietary, nursing, physicians, house staff, IT, media relations, research, etc. Team members had been identified and committed by June 1.

From previous experience, we realized the importance of not only adequately stocking essential supplies on-site, but also creating a back-up system to ensure additional supplies could be secured in times of an emergency. On Friday, we activated our supply chain and began to secure the additional supplies we had stockpiled offsite. Important supplies included: 400 flashlights; 100 head lamps; 2,000 batteries; 4,000 glow sticks, including 2,000 with lanyards; 600 SpectraLink wireless telephones with 1,800 batteries; 450 oscillating fans, one per patient; 250 box fans for work and sleeping areas; 20 55-gallon drums of water on each floor for commode flushing; 3000 gallons of water for drinking (we also have a deep water well on campus with a 10,000 gallon holding tank for additional water in an emergency); 60,000 gallons of diesel fuel; 10 pallets of sandbags; eight pallets of plastic bags; 100 blue tarps; 20 dehumidifiers; five pallets of plywood; and 50 additional shop vacuums. We also increased our food supply. At this time, we inspected our power sources. Our emergency generators are all located above our facility's second floor and our transformers were located on the ground level, behind 10-foot floodwalls.

On Saturday, August 28, executive leadership met with the vice presidents, directors, and managers and agreed to order Team A on-site by Sunday afternoon. Staff then began discharging the appropriate patients and moving those that would be unable to leave the facility. The families of the remaining patients were given "boarding rules"—one family member per patient would be allowed to stay. Similarly, staff was discouraged from bringing family members to work unless they absolutely could not make other arrangements. All patient and personnel families were pre-registered and given "special" parking passes to access our parking garage. Dur-

ing previous storms, we experienced problems with people in the community attempting to use our garage to protect their cars and boats. Under the revised plan, we stationed armed guards at the entrances to the garage to ensure that hospital staff, patients and their families could access the garage, and that all entrances were kept clear.

On Sunday, "sleeping" assignments were made. Due to concerns about the predicted high winds, patients were removed from the highest floors of the hospital. Patients were also moved into hallways and rooms without windows to protect them in the event of flying glass. Because OCF is a research facility, we house numerous research animals, which were evacuated to facilities in northern Louisiana. After evacuations were complete, we settled in to wait and see what Hurricane Katrina would bring.

Weathering the Storm

Ochsner's main campus survived the actual hurricane quite well. We sustained some roof and structural damage to our main facility, but overall the news was positive. Our generators functioned properly, the Internet was up and running, and our internal communications system was fully operable. Employees lost cellular phone and beeper capabilities due to damage to local cell towers; however, we had planned for such an event, and staff members were armed with SpectraLink wireless telephones. As a result, communication critical to patient care was uninterrupted. Our land-based telephones also remained in working order due to redundancy in our carrier network. Our medical record system is entirely electronic, and with power and the Internet operable, we did not have concerns about the availability of critical patient information. We had adequate supplies and believed we would be able to ride out the next few days.

However, as the situation in and around New Orleans rapidly deteriorated with the breach of the levees, conditions inside the hospital also took a turn for the worse. On the second day, one of our generators failed due to a mechanical problem, and we were forced to do without air conditioning. As a result, our Internet servers were shut down to prevent them from being damaged by the heat. Unfortunately, server shutdown meant the electronic medical record system was inoperable. We attempted to send our helicopter out to secure the needed parts for the generator, but all non-governmental aircraft were temporarily grounded. We were, however, able to locate the necessary parts the next day to get the generator up and running again.

Conditions in our immediate area continued to worsen. Our main facility is located a few miles from the I–10/Causeway where large numbers of people attempting to make their way out of New Orleans after the storm congregated. Many of those gathered turned to the hospital for assistance on their way. However, we are a hospital, not a shelter. We tried to point people in the right direction to get the help they needed, and also dispatched medical personnel to the site to care for individuals in need, transferring those needing hospitalization back to our campus. Conditions in our neighborhood further destabilized as floodwaters began to rise; looting of nearby businesses began. At that point, we felt compelled to ask the National Guard to assist us in securing the safety of our patients and staff, and placed OCF on lockdown.

Operations inside the hospital similarly were beginning to show signs of strain. Although we had made extensive plans for securing and relieving essential personnel with the Team A and B designations, and had gone to great lengths to keep staff apprised of the situation—setting up a telephone tree as well a dedicated Web page with information—we had difficulty securing relief staff. Many had evacuated with their families to Baton Rouge and beyond. Fortunately, we were able to locate a good portion of staff members there and bring them in by bus convoy. As the floodwaters continued to rise, the same convoys were used to evacuate exhausted staff and their families, as well as patients who could be moved and their family members, to our facilities in Baton Rouge. These same convoys were our lifelines for supplies as well, enabling us to continue functioning.

At their height, the floodwaters rose as far as the doors on one side of the hospital, but we maintained the ability to leave and enter the building from other entrances and faced no real danger. Instead, we realized that rumor and speculation were a larger threat to the internal stabilization of the hospital than the floodwaters, and created an internal communication system to keep staff and patients informed of the conditions within the hospital and the city at large. The leadership team met twice daily to be updated and then fanned out across the facility, sharing the news they had just heard and answering questions. This open and honest communication policy went a long way toward assuaging staff and patient fears, and keeping the hospital in a calm state.

Toward the end of the crisis, we began to run low on food. However, we had an ample supply of water and were able to make do until relief shipments could be brought in. We also ran low on insulin, but because our telephones had been unaffected, we were able to secure 10,000 doses donated from sanofi-aventis pharmaceutical company.

Reaching Beyond Our Walls

With the situation in OCF's main facility well in-hand, our leadership team sought to inform local officials and offer assistance to other health care facilities hit harder by the storm. Since our land-based telephone system was operable, we believed this would be easy. However, we had great difficulty trying to contact other hospitals and local agencies that were not as fortunate in the quality of their communications systems. We even found it difficult to locate the proper state and federal officials to offer our assistance.

According to our regional emergency plan, we report to the Jefferson Parish Office of Emergency Preparedness (OEP). However, the OEP system was overwhelmed and communication was impossible. When our attempts to reach the Jefferson OEP failed, we attempted to reach the Baton Rouge OEP. This was also challenging, as it appeared that the bandwidth of their system could not accommodate the high volume of incoming requests and was overloaded. We eventually successfully contacted the Orleans Parish OEP following the levee break, requesting both information, as well as assets. During this exchange, we became aware of their communications difficulties with the downtown hospitals that were in the midst of evacuating.

It was virtually impossible to coordinate air evacuation due to the various agencies involved—both military and civilian—and their lack of ability to communicate. We sent a vice president through the floodwaters downtown to the Orleans OEP with a hand radio to try and assist their coordination efforts, but were unsuccessful in reaching them. We instead found a widespread lack of coordination: police communication systems that were ineffective due to infrastructure damage and volume, and a National Guard system that was able to facilitate communications amongst guard units, but had difficulty communicating with local authorities. Of external communications, satellite systems were unreliable, and cell service, for a while, was virtually eliminated. Text messaging and Internet were the most reliable methods of communication.

Communication improved on day four when the United States Public Health Service (USPHS) arrived, and interagency daily meetings at OCF's main facility began. In addition to the USPHS, these meetings included "all" hospitals and representatives from the Jefferson and Orleans OEP health care divisions. The USPHS was able facilitate requests through the previously frustrating channels. They were particularly helpful with things like fuel and security; however, they did not have access to many of the assets we required. Prior to the USPHS's arrival, we were so frustrated in our inability to notify authorities that we were open and able to accept patients, that we used large trash bags to spell "OPEN" on our garage roof (see attachment A), hoping to attract the attention of the armada of helicopters flying overhead.

Assessing the Damage

Compared to our neighboring facilities, OCF weathered Hurricane Katrina well, and most aspects of our disaster plan worked as we had hoped. We sustained some structural damage on our main campus and lost three facilities. Our remaining facilities are stressed to their maximum. We currently are operating at 112 percent of inpatient capacity, and more than 50 percent of our staff has been displaced.

We are also revising all of our disaster policies in light of the events that transpired in Hurricane Katrina's wake. In particular, we are examining our family policy. Although we tried to limit the number of family members patients and staff could have at the hospital, we still found ourselves with more relatives than was optimal. We did our best to accommodate as many people as we could, and even set up a temporary kennel in the parking garage for pets. However, this added a great deal of complexity to our operations and was not accounted for when calculating the amount of supplies needed.

We are paying close attention to our generators and transformers. In the future, we will be sure to stock replacement parts for the generators onsite, so repairs can be made in a timely manner. We are also contemplating relocating the transformers to higher ground, despite the presence of a floodwall.

Our data storage system has also drawn scrutiny. As noted, we have a fully electronic medical record system. At the time Hurricane Katrina struck, we backed up those records at a location away from our main campus—in downtown New Orleans. Though neither location was jeopardized, we have secured a new location to house back-up copies of our electronic records. I cannot emphasize enough how important

our electronic records were. The system allowed us to instantaneously have the medical records available for our displaced patients who found their way to Baton Rouge.

We are very interested in ensuring that communication with the appropriate authorities and our colleagues across the area is maintained in the event of future emergencies. We weathered Hurricane Katrina and her aftermath as well as could be hoped for at our main facility. Because of the communication difficulties with the outside world, we knew we had to be self-sufficient, securing our own methods of sustaining our facilities. We were able to do this primarily because our facility in Baton Rouge could be used as an off-site command post, and our own communication systems remained operational. However, we could have done much more to assist the authorities and the local community if a fully interoperable communication system had been in place.

Conclusion

Mr. Chairman, the mission of every hospital in every community in America is to provide the best care possible to people in need. At no time is that more important than during a crisis, whether it be natural or man-made.

Hospitals across the country are doing their best to prepare for disasters that could strike at any moment. Many have become completely self-sustaining, capable of withstanding the most unimaginable crisis. But we cannot provide and help coordinate the care the community needs if we are islands unto ourselves. Communication with local, state and federal authorities is crucial for ensuring that hospitals can fulfill their mission to serve the health of the community during future disasters.

We look forward to working with this committee and staff to forge ahead toward to a shared goal of improving the disaster preparedness of America's hospitals and communities.

Mr. REICHERT. Thank you, Doctor.

Thank all the witnesses for your testimony, and now we have all the opening comments and presentations out of the way. We want to get to the bottom line.

First, I would like to just say a couple of things. September 11 and Katrina and Rita really shed a huge spotlight on this interoperability question. A few months ago, right before the break, we held a hearing on the topic of operability. We ca not become inoperable if we are not operable first. And so as we performed our jobs as first responders pre–September 11 and pre–Katrina, we experienced it in our own communities individual events that highlighted our inability to communicate with each other.

And then we tried to handle that within our community. I know that happened in Seattle in King Counties. Things would happen, we could not communicate, we tried to improve the radio system. We moved some towers, we moved some cell towers, et cetera. We tried to work with the companies providing the radios, and all of those things were going on in our own individual communities.

September 11 and Katrina highlighted this as a national problem.

Now, we need to look for leadership from the federal government, I believe, and, as I think most of you pointed out, from Congress in helping lead the way in setting some standards.

Some things have happened since September 11 in the federal government. There was recently enacted the Intelligence Reform and Terrorism Prevention Act, which does a number of things that we think are good, but, boy, we have a long way to go. It directs the secretary of Homeland Security to coordinate all existing programs. It establishes a national approach to achieving interoperable communications. It provides for technical assistance. It requires the states to develop a 5-year interoperability plan. All of those things are in the law, but they are not happening.

And the questions we have today is, why aren't they happening? And part of that, I think we are going to hear, is leadership is going to play a huge role. It is the turf wars that Ms. Linderman talked about. It is cooperation that needs to take place and relationship-building.

Lots of money has been spent. $2 billion already allocated, already out there in the pipeline on interoperability. $1 billion additional money has been allocated for interoperability grants this year, and more money is even authorized or placed in the budget, the upcoming budget that we are going to be discussing, $29 million more for interoperability. So things are happening in those arenas.

I would like to ask just very simply what the current state is. We have heard some of the issues, some of the problems.

I would like to hear from Trooper Perry. In Wisconsin, what is the current state of interoperability or the lack of interoperability?

Mr. PERRY. As every state, I am sure we share similar problems. Currently, our state has been working with a mobile data communications network to assist officers through writing their reports, crash reports, electronic citations, warnings, the gamut. With this communications tool, it is the in-car laptop computers. They are prevalent throughout the nation. We should be able to send a message to any other law enforcement in our state. We ca not.

And the reason being is we have 72 counties and not all 72 counties will play together and get on one statewide system. And it not only affects law enforcement, for instance, electronic reporting of a crash report. If it is not done electronically, it has to be done manually by someone else. Electronic citations, we send them in to what we call CCAP, Circuit Court Automated Program. That is the key; it is all automated. By sending it electronically, clerks in the Clerk of Court offices do not have to type the information manually from paper citations.

The area that I live, Green Bay, and the counties that I work, Brown, Outagamie, Winnebago and Calumet, those four counties decided that they had a better way of doing things and they would create their own mobile data system. So they are not operable with the other counties, they are not operable with all the law enforcement within those counties.

They cannot print electronic citations, electronic crash reports, because they spent their money on getting their system up, what powers communications for their plant form. Now they have no money to write the software. Now they have to go back and get more money from state and federal tax dollars so they can write programs so they can begin the process of electronic citations, for instance, when it was available, and it still is available, if the political leaders would get on board and say, "Look, it is time to play with the other communities throughout the state."

We also see it in communications. If it was not for the industry private sector, often officers throughout this nation would not have communications. Police officers, deputy sheriffs and troopers throughout this nation are not all issued a cell phone. I use my cell phone religiously. I carry it with me. That is the first thing I put in my shirt pocket after putting my protective vest. Those are the

two most important things I have each day beyond any of the other equipment I carry on the belt.

The last car fire I was at was on a freeway. Our portable radios are so out of date, our technicians cannot purchase rechargeable batteries from the vendor. They actually go to Radio Shack and build a rechargeable unit for us. Last fall, they were behind in car swaps and putting in new equipment and IT radios to run the mobile data communications network. They did not have time to build those batteries, so during a 3-month period my portable batteries would run out within 1 to 2 hours. So with having issued two to three of them, I was out during my shift.

Not only was officer safety compromised, but at this car fire on the freeway where I have to shut down the highway using city of Kaukauna police officers, Outagamie sheriffs deputies, state troopers, I also have to call fire. It would have been extremely embarrassing, and I know would have had the political fallout from my own Department had I dialed 911, but that is what I should have done and maybe I would have gotten some action.

Instead, I had to call my dispatcher, get through her and then ask her to call fire, ask her to continue to stay on the line so we could coordinate getting the traffic off the freeway and around the community so that we could take care of the fire, put it out, have a tow truck respond, tow it off so we could open the freeway once again.

Mr. REICHERT. Thank you. This is the kind of information that we are looking for, the people that are actually out there doing the street, and I appreciate you being here today, Trooper.

One of the things—and what you have described is something that is happening in the area of the country that I come from too, so it is not a surprise to me that you described your state of affairs the way that you did.

I am going to ask a real quick follow-up question. You know, we changed the definition of "first responders." Now it includes all of you at the table. We know that we have to take a broader look at that.

I am just interested to hear quickly from Dr. Pinsky and Ms. Linderman. Are you able to include yourselves, your associations, in the discussion with first responders, and are you having some success in the areas of the country that you come from in building those partnerships, including your groups in the discussion around being interoperable?

Mr. PINSKY. I can probably answer that from a couple different directions. Number one, we are now working much more closely through the local hospital association, the Metropolitan Health Council, as well as the Louisiana Hospital Association with our fellow hospitals to be sure that we can establish communication among ourselves.

Because we found that Katrina that we were unable to communicate with each other. Our Internet function stayed up because we had multiple ports. We have a very large wide area network. The other hospitals did not have that redundancy, so we could not communicate directly to them.

We have also had conversations now, we have had meetings now with the local first responders to improve upon the situation that

we had. Our biggest difficulty in New Orleans right now is that we have not recovered from Katrina yet, and so we are still dealing with all of those issues, at the same time trying to prepare for the new hurricane season in 3.5 months.

Mr. REICHERT. Thank you.

Ms. LINDERMAN. As Trooper Perry talked about Wisconsin, I was reflecting on our membership, and the situation across this country is different in every community. Richmond has the advantage of having the leadership within the region to, with local tax money, implement regional communications system that would work. But there are many communities and members in our organization that did not have that leadership at their local level.

So it is going to vary all over the board depending on who is helping to make the decisions, who is pulling together the different agencies to be able to communicate.

There are still challenges as you go up through the government strata. In local government, there can be decisions made that force communications among agencies, but as you get into the state and federal level and interoperability between those different levels of government, I think there is still a challenge.

Certainly, APWA is trying to help our members to be more knowledgeable and educated so that they can take a stronger stand in their local governments or in their state governments in order to make interoperability happen.

Mr. REICHERT. And, Mr. Moroney, I did not want to ignore you on this one, but, certainly, you have a comment. Please.

Mr. MORONEY. I think that when we look at what is being done in the market, I struck by your comments about how a billion dollars is being spent. Ours is an industry that spends $1 billion a year just building wireless systems, upgrading existing wireless systems, and they are all over the block. Because nowhere in our country is there a single place that they can work, that they can build a wireless system that is interoperable with other parts of the country.

In terms of your question about how is it going in terms of working with the other communities, I think it is not going as well as it could. In some areas, you find great models. I look to the state of Missouri that is proposing a statewide interoperable communications system and all emergency first responders are included in that.

I look at the state of Mississippi during Hurricane Katrina and one of our members, the Southern Company, had a communications system that was used by a number of local first responders as well. And it was a system that stayed up and running following the hurricane.

So it is very spotty, and I think it was Trooper Perry who said, "You all have told the rest of government what it needs to do, and maybe now it is time to take their allowance away or something."

Mr. REICHERT. Thank you.

The Chair recognizes Mr. Thompson.

Mr. THOMPSON. Thank you very much, Mr. Chairman. I think it is quite clear that we still have a problem. All of the witnesses have, in their own words, shared their horror stories around the problem.

What we have had is a difference on how we approach it. My own state, Mississippi, has indicated that it will cost us $300 million to design a system statewide. So a billion dollars does not go very far when you are investing $300 million in one state alone. So we are talking about a significant investment.

Another one of our challenges associated with investment is to what extent are we using the latest technology to allow the notion of interoperability to be satisfied? My experience is that many times the vendors are selling their products to individual departments as the savior for what happens. So, in essence, you are putting up towers, you are buying radios, but you have not solved the problem of interoperability, because you now have new equipment for the police department but what does that do for the fire department, what does that do for the public works department?

So the notion is to acknowledge it has to come into play at some point to facilitate this communication.

Mr. Chairman, I think what we will have to do, taken this testimony, is to see how we can provide the leadership, so rather than becoming the purveyor of radios, how do we deal with the technology so that people can communicate? And that is a real challenge.

To what extent, and I guess Mr. Moroney, you can help me with this piece, do you see technology providing the breakthrough for interoperability?

Mr. MORONEY. I think technology is one answer, part of the answer. One of the problems we all face with technology is we are all either public institutions or we are regulated commercial companies, like utilities, in which all of our costs get passed through the citizens. And so we are still looking at building radio systems, interoperable or not, that are going to last for 10 years. Technology is changing so rapidly that 6 months after we agree on a technology there is a better one out there.

One of the things that we need to be able to look at is, how can we better fund the adoption and use of new technologies?

Another part of the answer is not just technology, it is when I look at every plan that I have heard mentioned here today about communications. When your state looks at building a system for $300 million, they are talking about a big part of that cost is the infrastructure necessary to support it—the towers, the fiber back hall, the computer systems that will manage the voice and data traffic—and it is going to be built right alongside another set of infrastructure.

If we could look where we have seen success with shared systems is where a whole group of emergency responders collectively invest in building the same infrastructure, and then the cost of providing additional handsets, the cost of providing additional laptop computers and additional communications becomes much more reduced when you have that huge infrastructure cost shared by all the participants.

So it is a combination of technology. If you shared the infrastructure and invested in adapting new technologies to that infrastructure, we could take advantage of newer technologies more rapidly.

Mr. THOMPSON. Well, you know, one of the things that I think we have to do is mandate the cooperation and coordination between

entities. So many times we have cities who are on radio systems and counties or parishes who are on another, and they are somehow helping the same citizens but they ca not communicate. And we have to break down some road barriers to facilitate the communications.

Now, I think that is where Congress can play a significant role by saying, "If you agree to take the money, then you agree to communicate and cooperate with each other in a time of need." And as I see what is occurring, I see what you are saying, but we have to provide the additional leadership to facilitate the cooperation and communication, and that is where I see this bipartisan legislative effort, which will get us there hopefully, and that is why your testimony adds significantly to what we will ultimately come up with.

I yield back.

Mr. REICHERT. Thank you, Mr. Thompson.

The Chair recognizes Mr. Dent.

Mr. DENT. Thank you, Mr. Chairman.

To Trooper Perry, I want to address my question to you. In the state of Pennsylvania where I live, we have 67 counties, 2,500 municipalities and 501 school districts. Suffice it to say, we have turf issues, very serious turf issues, and I was struck by your testimony where you said, "The parent needs to withhold its children's allowance, or in this case federal grant money, until they learn to cooperate with each other."

I think Ranking Member Thompson kind of alluded to those issues, and maybe as a federal government we can play a role. I am not so sure a mandate will help, but, certainly, withholding money will get some people's attention.

You also mentioned we need to overcome the political issues across jurisdictions, that states must be—the federal grant money needs to come with strings attached. You get into the issue, too, of states redistributing federal grant money to county and municipal governments, must be sure that that money is spent on compatible equipment and software when we are faced with a statewide platform.

I would also note, too, that I recently met with my regional counterterrorism task force in southeastern Pennsylvania, which is Philadelphia and four surrounding counties, a region of about 4 million people. And I was impressed by the fact that they were largely interoperable, and that is the question, all but for about four or five municipalities, which in that part of the world was pretty good. So I was pleased by that.

Then you also talked about the lack of common standards among vendors. It continues to present difficulties for interconnection, and your bottom-line assessment was that federal tax dollars are not being allocated, managed or spent efficiently.

So I guess my question to you is, knowing that we have spent all this money on interoperability, is this really more a problem of—is this a money problem or a coordination and accountability problem when you get right down to it? That is my main question.

And, finally, I think you also illustrated the problem quite well with your disclosure requirement statement, and I am just curious, your program was to receive $211,000 and to date the NTC has not drawn down any of that funding. And I take that this grant was

approved in 2003. Can I ask why that money has not been drawn down?

Mr. PERRY. Yes, sir. In putting together this study, we decided that it would be better appropriately for our organization to create another corporation that we could serve for research and training. And we are waiting for approval for that final one.

Mr. DENT. So you are ready to spend the money but you can not get an approval?

Mr. PERRY. No. The money is approved. We were internally adding another corporation to our branch of the Troopers' Coalition so we could better serve that under education, training, and that is why we wanted that grant money to go into that corporation so that we could do this appropriately.

Mr. DENT. Okay. Because, again, in a state like mine, much of our terrorism preparedness grants have not been drawn down, for whatever reason, one of which I just met with a large fire department in my district, municipal fire department, city of Allentown, where they cannot draw money down, and they ca not get purchase orders processed. That is at the state emergency management agency so that they can draw down funds or they are desperate, they need it right now. So I am glad to hear that is not the case with your grant.

Could you just please address this question of, is this really an issue of money or is it more of an issue of accountability and coordination?

Mr. PERRY. I think that it is money and accountability coordination. More funds have to be allocated for this because of the amount of technology that is constantly changing and putting that infrastructure throughout the state that the users can then operate off. But when we come into the accountability, politics does play a role. The money from the federal government goes to the state, and sometimes the money going into the county or the municipality sometimes there is politics involved here. That is where the problem comes in.

Sometimes you will have the squeaky wheel gets the grease, so to speak, and if one region is very political and has the ear of the person in charge of redistributing the state grant money, that is where that money is going to go, whether it is going to be compatible to the state's system or not.

Mr. DENT. And should we be looking at—and maybe Mr. Moroney or somebody else could comment on this—I remember the Philadelphia region doing a reasonably good job on interoperability, interoperable within southeastern Pennsylvania where also part of that region includes portions of southern New Jersey and the state of Delaware.

And maybe we need to look at this more on a regional basis. The same thing can be said in the New York metropolitan area: You deal with New York and New Jersey and Connecticut.

Anybody have any thoughts on that issue?

Mr. MORONEY. It would be wonderful if we could come up with one totally interoperable, totally shareable communication system used by all emergency responders nationwide. I think practically anybody here at the table could tell you what it ought to look like and what it ought to do. I have no idea how we would get from

here to there. So your suggestion that regional approach is this is going to be a series of steps that are taken.

But I think some of the steps are not just looking at it from a regional point of view of where there is the political will to do it. It is going back to providing the incentives necessary to get it done. And maybe it is not so much withholding the allowance, it is putting a carrot out there.

And there are a number of ideas. Our suggestion of saying to the utility industry to allocate a certain amount of spectrum, not spectrum that is currently being or already been allocated to traditional public safety, is a carrot, and you say, "Here, if you use this spectrum to build communication systems, you must build a system that is then shareable by all emergency responders in an emergency or you must do this with it. If you do not do that, you ca not have it." That is the kind of a carrot that would provide an incentive, because there is already a financial incentive for our companies to move toward that.

And I think the same is true for kinds of incentives for political entities to support traditional public safety.

Mr. DENT. Thank you.

Mr. REICHERT. The Chair recognizes Ms. Christensen.

Mrs. CHRISTENSEN. Thank you, Mr. Chairman, and thank you for holding this hearing.

I want to thank the panelists particularly for your recommendations. It has not been a question that interoperable communications is a necessity, but the recommendations are very important, and I think that we can in this committee move in a bipartisan way to respond to some of what we have heard here this morning.

I want to direct my question, at least if I get more than one out, I will move around, but first to Dr. Pinsky. And I ought to commend Ochsner and their good work. As I was reading the testimony last night, I was going, "Wow, they really did a good job," until I got to whatever page that was and you tried to communicate outside. Everything was just flowing perfectly.

But I am not sure whether that was because of citywide planning and maybe some statewide planning and exercising or in spite of it. So I have three questions, and I am going to ask them all at once so I can get them out.

Prior to Katrina, were you a part of the planning and the exercising of the city's Emergency and Homeland Security Preparedness Council or whatever it is called there?

And was there exercising with other hospitals, the public health system and private physicians?

I would like to know from the American Hospital Association perspective if you feel that there is enough involvement of hospitals and public health and planning.

The electronic medical records, do you consider that an integral part of interoperable communication when we talk about homeland security? I am always curious also as to how much in hospital preparedness funding did Ochsner get from the Department?

Mr. PINSKY. Okay. I will start with the second question first, which was in regards to the electronic medical records. We have an electronic medical record with all of our patients' data on that. If

there was ever any question of whether investment in electronic medical records was worth it, this answered it.

With so many of the patients being—virtually the whole city being displaced, a large number of those patients, individuals ending up in the Baton Rouge area where we have facilities, we were able to make patient information available immediately. Or if the patient had relocated to Houston or somewhere else, a physician in the other city could call us and we could make available the information immediately.

It was very important, and I suppose that is another form of interoperable—

Mrs. CHRISTENSEN. I think so.

Mr. PINSKY. —communication.

As an adjunct to that, because we are an academic institution, we have a large number of patients who were part of clinical trials and research. In fact, many of our cancer patients, many of our heart patients depend on these trials for their regular care. Because of the electronic medical record in our databases, we were able to have that data available as well and be able to set up communications for these people to contact us.

That is the part that many times is overlooked when we talk about the delivery of health care.

The funding of our electronic medical records, the funding of our own internal emergency preparedness comes from our own budget. We, like many hospitals, have a significant number of Medicare patients. We probably had prior to Katrina about 50 percent of our discharges in the hospital were Medicare patients. On top of that, we have a significant amount of Medicaid patients. And now post–Katrina, the number of uninsured patients has quadrupled.

So when we talk about our hospital, and I think hospitals as well, ability to fund their activities, obviously our payment sources are critical. So every change, every tweak that goes into the Medicare plan or goes into Medicaid plan hurts us in terms of ability to be able to, a, keep our doors open and, b, be able to fund these other activities.

Mrs. CHRISTENSEN. Participating in the planning.

Mr. PINSKY. Prior to Katrina, even though our planning was very intense internally, it was not integrated into the rest of the area. We did meet with the Jefferson Parish emergency office and had updates and had the data that they had produced in terms of the modeling of the effects of the hurricane but not in terms of going through a mock hurricane disaster, city or region-wide.

I can tell you that the American Hospital Association feels this is very important for us to be doing, and that is why I mentioned earlier our involvement with the other hospitals, particularly locally in terms of the city, which is the Metropolitan Council, and then statewide is going to help facilitate for us going forward.

Mr. REICHERT. The Chair recognizes Ms. Harman.

Ms. HARMAN. Thank you, Mr. Chairman, and thank you for holding this hearing.

Congressman Etheridge is no longer here, but I do appreciate his reference to H.R. 1646, the so-called HERO Act, which adds a critical dimension to this problem. And just for the record, I want to

remind our committee and our witnesses of what this bipartisan bill has been after for the several years since its introduction.

What it has been after is to keep the promise Congress made 10 years ago to free up analog spectrum for emergency communications by the end of this calendar year, 2006.

The promise, as many of the promises he made, contained a loophole. That loophole was that this would only happen if 85 percent of the broadcast channels had transitioned to digital broadcast, and since that has not happened, the promise is not happening.

But I think a lot of what has been discussed today could be substantially alleviated if there were national dedicated spectrum for emergency communications. And I think the resistance for this idea, which comes from the broadcast community, is enormously shortsighted, because those folks live on the same pieces of real estate that the rest of us do, and they, their families, their children and their uncles and aunts and other friends are at the same place that the rest of us are in the event of a manmade or natural disaster.

So I want to call one more time for Congress to review this issue. It is true that we acted last year, not in this committee but the full Congress acted, to transition analog spectrum by February 2009. Everyone should get it that that is 3 years from now, and I do not think the next Katrina or the next al-Qa'ida assault is going to say, "Ooh, let's wait until February of 2009."

So I think we are doing the wrong thing. This subject is not in this committee's jurisdiction, but this issue is in this committee's jurisdiction, and on behalf of the many members of this committee who are co-sponsoring this bipartisan legislation, I would like to send a message out and about that we should not back off. The broadcasters should back off.

At any rate, I do not assume I have any disagreement from the panel, but I thought that that rant might be useful.

I want to say, Dr. Pinsky, that you performed a great service to the communities you serve during Katrina. I think we either should have you or a clone of you in charge of FEMA and our national strategy. Clearly, there is a lot of room for improvement, and you bring a learning curve that is very valuable. So on behalf of the constituents of the 36th district in California, I thank you for what you did.

I just want to make a general comment and get your reactions. And that is that in addition to spectrum, the other big pieces, at least that we can contribute, are a national strategy, which we do not have, and standards, which this committee is working on and can work on within our jurisdiction.

I just want to ask you folks whether you agree with me, at least from the federal perspective, that spectrum, strategy and standards are the three S's at arriving at a true national interoperability capability and that Congress should move faster?

Ms. LINDERMAN. I would agree that those are certainly very important for us, but the challenge is going to be figuring out—many communities have made investments in their systems and how you do not throw that away with the bathwater. We have to figure out how to make that work.

The standards, I would suggest in the development of standards that there is a representation, certainly, from local governments, state governments and federal governments, to make sure that those standards can be implemented successfully.

Ms. HARMAN. I agree. And part of the problem is in the vacuum localities have done whatever they could do to at least make certain that they can talk to each other. That is not true in every locality, and, clearly, there was a massive breakdown in New York and at the Pentagon on 9/11. We all understand that.

And so I salute you for your efforts. We do not want to throw out the baby with the bathwater. On the other hand, we do want to provide more guidance quickly so we do not have interoperable capabilities in various parts of America that are not interoperable with each other.

I see my light has turned red, but I am sure the chairman will give me permission to hear from the others in response to my question.

Mr. REICHERT. Absolutely. In fact, if you have an additional question, feel free to ask.

Mr. BRADLEY. I would just like to say that those are certainly the three critical issues, and one of the most critical to me would be that the standards are complete before the spectrum is available. If not, there will be a lot of work done on the spectrums by people who are interested in getting on it immediately. It will not meet the rest of the individuals when they come on board. So I think the standardization needs to be done very rapidly before the spectrum is done.

Mr. MORONEY. I could not agree more. I would just suggest or remind that one of the things that I think is critical in either the strategy or the standards is that those interoperable systems be built in a manner that they can survive a disaster. Terrorist attacks or hurricanes tend to take out the power, and the best interoperable system that no longer has power supporting it ceases to function, and interoperability is not the issue.

And as I said in my testimony, utilities do build systems this way, and so including them and their systems and how they build them in a strategy we think is essential to interoperable systems that continue to interoperate during emergencies.

Mr. PERRY. I agree also on the standards. It has to be a priority. I also want to reemphasize that not only is the big picture the next disaster important, first responders face this interoperability compatibility issue daily. This is where we need immediate help is on the day-to-day activities of all the first responders. Thank you.

Ms. HARMAN. Thank you, Mr. Chairman. I think these are folks we should be consulting as we move forward on this issue. I think their testimony was enormously valuable.

Mr. REICHERT. Thank you.

Ms. HARMAN. Thank you for accommodating my extra time.

Mr. REICHERT. You are welcome.

Ms. Christensen, do you have additional questions?

Mrs. CHRISTENSEN. I did have a question based on something that Mr. Bradley had in his testimony regarding the administering of the spectrum by NTIA and your concern that it perhaps would be better under the Department of Homeland Security.

So I wonder if you would comment on that and if anyone else had an opinion?

Mr. BRADLEY. The administering of the grants is a critical issue and dealing with the first responders I think DHS has a better relationship, has better experience in the past in dealing with grants or doling out grants to first responders agencies.

There is a myriad of first responders agencies. They often are confusing to those who have not dealt with them, the structure, the relationships between them. And of course the consensus or the standardization of getting all of them working together is important, so I think we believe that DHS is the appropriate agency to administer.

If it is not administered by DHS and is transferred or kept in NTIA, then we think that it ought to follow the guidelines in the SAFECOM report or the SAFECOM requirements for the distribution of funds for communications.

Mr. REICHERT. I have a couple of additional questions.

First is for Mr. Bradley. Has the fire profession, volunteer and full-time, undertaken a national operable communications needs assessment that you know of?

Mr. BRADLEY. Not to my knowledge, Mr. Chairman, other than working through or following the guidelines of SAFECOM.

Mr. REICHERT. I guess I want to take a moment here just to kind of sum up what we have kind of heard. And I also want to take a moment to reinforce the statement that Mr. Pascrell made. We are going to get this done, and, as I said in my opening statement, this is a subject that is near and dear to my heart after 34 years of doing the job that Trooper Perry has done for many years.

You know, we can share life and death stories about the failure of our ability to communicate with each other, and some are so dramatic that we wonder why. And in my own career, I think back, why haven't we done something yet? And as I said earlier, September 11 and Katrina pointed out the severe weaknesses in our ability to communicate across this country.

There are a few things I think that are key in our success as we move forward, and today what we want to ensure is that we continue to have dialogue with all of the people here this morning who have testified.

You are the experts in the field. You are the ones using the systems or not using systems that are not available right now and see the weaknesses. We need to know about those. We want to keep in touch with you.

But some of the things that I have heard today really are leadership management. It is about accountability, and I like to kind of equate that to really having some performance measures in place so that when money is allocated and the people do start to build a program, to build an interoperable system or first an operable system, that much like COPS office operates, and I know because I have over my years had a great partnership with the COPS office. They have a system of accountability and performance measures already in place that I hope the Department of Homeland Security would view as one that they may be able to adopt.

The most important thing I think that needs to happen here, and I think I have heard it from all the witnesses and from the mem-

bers of our committee, is that there is no priority higher right now in the protection of our country and our ability to respond to emergencies, both natural and manmade and interoperability. And right now this administration and the Department of Homeland Security has not made interoperability a high priority, and we intend to change that.

And this committee, as you can see, this is not a partisan issue, this is an issue that we all come together on. So we are with you, and we are going to make this happen.

I want to thank you all for your testimony, and our committee hearing stands adjourned. Thank you.

[Whereupon, at 11:46 a.m., the subcommittee was adjourned.]

THE STATE OF INTEROPERABLE COMMUNICATIONS: PERSPECTIVES FROM STATE AND LOCAL GOVERNMENTS PART II

Wednesday, March 1, 2006

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON EMERGENCY PREPAREDNESS,
SCIENCE AND TECHNOLOGY,
Washington, DC.

The subcommittee met, pursuant to call, at 2:05 p.m., in Room 311, Cannon House Office Building, Hon. Dave Reichert [chairman of the subcommittee] presiding.

Present: Representatives Reichert, Dicks, Harman, Lowey, Norton, Etheridge, and DeFazio.

Mr. REICHERT. [Presiding.] The Committee on Homeland Security, Subcommittee on Emergency Preparedness, Science and Technology will come to order.

The subcommittee will hear testimony today from state and local governments on the state of interoperable communication.

I would first like to welcome our witnesses and thank them for being here today, and thank you for taking time from your busy schedules.

And before we get into opening statements, Mr. DeFazio from Oregon has asked unanimous consent to introduce the Honorable mayor from Beaverton.

Mr. DeFazio?

Mr. DEFAZIO. Thank you, Mr. Chairman. Thanks for allowing me to move ahead.

This is an issue of tremendous concern for me, and I know the committee will do a good job today. Unfortunately, we also have a hearing on a critical regional issue, our Bonneville Power Administration, which I have to go to.

But I was particularly anxious to introduce Mayor Drake, the mayor of Beaverton, Oregon, today, because not only has he been a great mayor for that city for more than a decade now—Rob, we have been doing this for a long time—but he has extraordinary expertise in public safety issues. And he will be a great witness to represent the local perspective on the need for interoperability and what the federal government can do better to partners.

Chair of the regional emergency management group since 1993, he is a member of the Public Safety and Crime Prevention Steering Committee with the National League of Cities, and he represents

National League of Cities on the Department of Homeland Security's Project SAFECOM Executive Committee.

So I think that his input, and I know the other witnesses, will be extraordinarily valuable.

And, again, I thank you, Mr. Chairman, and I hope that today's hearing marks further progress on interoperability, which we need so critically.

Thank you.

Mr. REICHERT. Thank you.

Let me welcome you again, and on behalf of the members of the subcommittee, we are glad that you are here to share your experience and knowledge with us. Your leadership in trying to solve the problem of emergency communications in your perspective jurisdictions distinguishes you, and we look forward to hearing from you today.

The purpose of this hearing's second series on interoperability is to understand the state of public safety interoperable communication from the perspective of state and local governments. Public safety interoperability begins with you, our state and local partners.

You own the majority of our nation's public safety communication systems. Your fellow citizens must live with the consequences of your successes or failures. And you are in the trenches day in and day out trying to solve this problem. That is why your perspective is so valuable to us.

Public safety is among the most basic and critical of the services coordinated, regulated and funded by state and local governments. Yet when our nation's first responders lack the ability to relay mission-critical information to each other on demand and in real time, everyone's safety may be needlessly compromised.

Unfortunately, in many jurisdictions, public safety agencies still operate and maintain largely independent emergency communication systems. Such stovepipe communication systems generally lack the capacity to support interoperability with the surrounding federal, state and local agencies. But interoperability, by definition, requires coordination among and partnership between all levels of government.

It is clear that the problem of public safety communications cannot be solved by any one jurisdiction alone. That is precisely why federal, state and local officials have begun to establish state interoperability executive committees and regional interoperability committees, councils and/or workshops.

Such high-level coordinating and rulemaking bodies play a vital role in helping state and local officials improve public safety communications. And they provide badly needed venues for planning, policy development and fostering interagency relationships.

In mid–February, this subcommittee received testimony on interoperable communication from first responders. From each and every witness we heard the same thing. We heard about the need for consistent leadership, not for billions of dollars in additional funding, but for policy makers and government to simply work together.

The members of this subcommittee have heard that message loud and clear, and as its chairman and a cop of over 33 years, I intend

to make sure that Congress does its part to help federal, state and local officials implement a unified approach to the problem of emergency communications.

I want to thank the witnesses again for their testimony.

And the Chair will now recognize—would recognize my friend from New Jersey, but he is not here, tied up on other business. I will recognize Ms. Harman from California.

I would like to acknowledge the bipartisan spirit of this subcommittee. Today's hearing marks the first time that any subcommittee of the Committee of Homeland Security has distributed to members a bipartisan briefing memo drafted jointly by both staffs. It is an important precedent that I would like to continue in the future with Mr. Pascrell's consent, of course, and assistance.

And I know we often talk about working together, but I hope that this sets an example and shows my intention to work cooperatively on issues of national importance. Quite frankly, how can we expect state and local governments and emergency providers and others to work together to solve the problem of interoperability if we do not practice what we preach?

I look forward to continuing to work on a bipartisan basis with my colleagues and so now yield to Ms. Harman.

Ms. HARMAN. Thank you, Mr. Chairman. I applaud the remarks that you just made. I often say that the terrorists are not going to check our party registration before they blow us up. And so it is absolutely imperative that we work together to fix at the federal level what I think are two huge gaps in our homeland security. One is, the lack of a national integrated strategy. We are doing better but we have a long way to go.

And the second is, the lack of true interoperability. I see these witnesses nodding and I see our colleagues nodding. The folks in this room, on this committee, have been dedicated to fixing this problem for a long time, and we have not, at our level, gotten very far.

So that is why I want to congratulate the dedicated public servants in front of us who are doing everything they can at the local level to make certain that when they have both natural and manmade disasters, they have the ability to talk to each other.

Just speaking for my region of California, the largest county in the United States, Los Angeles County, my local first responders and law enforcement personnel have figured out some bridging technologies that give them the ability to drive a flatbed to the site of a problem, and on that flatbed are a series of ACU–1000s, which are a device to grade a number of frequencies.

Now, that is great if the flatbed can get there. But in the case of a fire where the roads are out and the heat is too high, I mean, we still literally have people having to drive around the entire fire, swap radios and so forth, and we are are obviously in a dreadful mess in those situations.

So I do not think we need another Katrina or a catastrophic terrorist attack to tell us how serious this problem is. I think what we need is more action at this level.

Some of you, I assume all of you, know that I have coauthored the HERO Act with Congressman Weldon, who is another member of this committee, which would require that Congress keep its

promise for dedicated spectrum by the end of this year. Sadly, HERO has not become law. The promise Congress is now making is to move that date to sometime in 2009. I think that is inadequate. But the good news is what you are all doing and also the fact that there are new technologies out there—I just heard about one—that may be able to get this job done without the need for dedicated spectrum. And if that pans out, we may be able to solve this problem faster.

Let me just conclude, Mr. Chairman, by saying that the Homeland Security Department itself, sadly, is no longer funding the COPS Interoperability Grants Program on the grounds—or the government is not, on the grounds that the program is redundant with what Homeland Security is doing. But Homeland Security does not have a dedicated Interoperability Grant Program. So that is unsatisfactory.

And I think if there is a short-term future, we are going to hear it from our witnesses, and I just want you to know that on a bipartisan basis the members of this committee want to help you achieve something in our national interest.

Thank you, Mr. Chairman.

Mr. REICHERT. Thank you, Ms. Harman.

Other members of the committee are reminded that opening statements may be submitted for the record, and we are pleased to have with us today a distinguished panel of witnesses.

The first is the Honorable Rob Drake, mayor of the city of Beaverton, Oregon, and member of the National League of Cities, Public Safety and Crime Prevention Steering Committee. Next is the Honorable Gino Menchini, commissioner of the New York City Department of Information Technology and Telecommunications. And Chief Charles Werner, fire chief of the city of Charlottesville, Virginia, and member of the Virginia Statewide Interoperability Executive Committee. And Mr. Steve Proctor, executive director of the Utah Communications Agency, former national president of the Association of Public Safety Communications.

Let me remind the witnesses that their entire written statement will appear in the record. We ask that due to the number of witnesses on our panel today, that you strive to limit your oral testimony to 5 minutes.

And the Chair now recognizes the Honorable Mayor Rob Drake.

STATEMENT OF ROB DRAKE, MAYOR OF BEAVERTON, OREGON, MEMBER, AND CRIME PREVENTION STEERING COMMITTEE, NATIONAL LEAGUE OF CITIES

Mr. DRAKE. Thank you and good afternoon, Mr. Chairman, Ranking Member Pascrell and distinguished members of the subcommittee. My name is Rob Drake, and I am the mayor of the city of Beaverton, Oregon.

Today, I am testifying on behalf of the National League of Cities where I serve as a member of the Public Safety and Crime Prevention Steering Committee. I also represent NLC on the Department of Homeland Security's Project SAFECOM Executive Committee.

Interestingly, today marks the third anniversary of Department of Homeland Services, and NLC's wish is for the Department to make greater strides on interoperability. For many communities

and regions around the country, the challenge of interoperable communications represents an immediate threat to the viability of their public safety operations.

In my hometown of Beaverton, which is part of the greater Portland metropolitan area, we approach interoperable communications from a regional perspective because public safety is an issue that does not respect political or geographic boundaries.

I have served as chair of the Portland Area Regional Emergency Management Group, REMG, since 1993. REMG is the vehicle by which the public and private sectors in the Portland–Vancouver region work together to organize, plan and define regional needs and develop common policies and procedures to follow in the event of a disaster. The group is dedicated to providing a long-term model for regional coordination and planning, driven by operational necessity, not by financial incentives.

This is a voluntary group, formed through intergovernmental agreements between special districts, city, county and regional agencies in the five-county, bi-state, Portland–Vancouver metropolitan area. It includes the American Red Cross and steady participation from utility providers and local and global businesses.

Some key initiatives for REMG include identification and publication of regional emergency transportation routes; development of the greater Portland–Vancouver area emergency alert system, EAS Operation Plan, in coordination with broadcasters across the region; development of a regional disaster debris management plan in cooperation with Metro, Portland's regional government and local solid waste program managers; voluntary agreement between local governments to address emergency management issues for the benefit of the entire region, regardless of resources or participation in the group; staff deployment from participating agencies without compensation to work with the regional partners; and, finally, involvement of policy-level representatives from each signatory agency who provides structure to the group and assists in developing sound policies and procedures for use in disaster situations.

REMG works effectively because its signatories agencies believe in the value of a regional plan, which ensures the integration of all individual plans under the umbrella of one common plan.

There are many advantages to coordinated emergency response. First, it develops proactive relationships between likely co-responders. Second, it brings together from across our region a collective knowledge for the benefit of the entire region.

Third, it reduces duplicate efforts, which helps identify and allocate finite resources, maximizes resource utilization and ensures communication of a consistent message to our public. Congress should support mechanisms that encourage coordinated planning on a regional level.

The challenge of integrating levels of service provision is daunting. I have helped guide regional cooperation among local officials for the last 13 years. It has taken very hard work and commitment to keep this on track.

I would recommend the following to strengthen the federal role on interoperable communications.

One, elevate the visibility of Project SAFECOM. Project SAFECOM at Department of Homeland Security is a great example of a federal agency incorporating the input of local governments to improve interoperable communication plans and guidelines. Elevate the visibility of Project SAFECOM and its mission, because interoperable communication influence hometown security directly.

Two, build on the spine of existing communication networks. The federal government should design programs that benefit first responders at the local level but within a national scheme. Build on the spine of communication networks that promote enhanced public safety and disaster response capabilities across multiple jurisdictions.

Three, funding flexibility. NLC urges Congress to allow more flexibility in the use of federal public safety funds for upgrade technology communication systems and training. The federal government should provide funding directly to local governments for homeland security, emergency preparedness and response because we are the initial focal point of all disaster mitigation and recovery activities.

The fourth point, federal government should commit to date certain for return of analog spectrum. While NLC acknowledges the political challenges that led to a date certain return of analog spectrum by February of 2009, NLC reminds Congress that more lives than necessary may be lost between now and then because of the lack of spectrum. NLC urges Congress to lead efforts to accelerate, if possible, efforts to resolve interoperability problems that affect emergency communications and data systems throughout the nation. No one should lose his or her life because public safety officials cannot communicate with another.

Thank you, and I would be happy to answer any questions.

[The statement of Mr. Drake follows:]

PREPARED STATEMENT OF HON. ROBERT DRAKE

WEDNESDAY, MARCH 1, 2006

Good afternoon, Chairman Reichert, Ranking Member Pascrell, and distinguished members of the subcommittee. My name is Rob Drake and I am Mayor of the City of Beaverton, Oregon. I have served as mayor since 1993. We are a city of 83,500 citizens and touch Portland on its west side. I am testifying today on behalf of the National League of Cities ("NLC"), where I serve as a member of its Public Safety and Crime Prevention Steering Committee. I also represent NLC on the Department of Homeland Security's Project SAFECOM Executive Committee.

NLC is the country's largest and oldest organization serving municipal government, with more than 1,800 direct member cities and 49 state municipal leagues, which collectively represents more than 18,000 United States communities. Its mission is to strengthen and promote cities as centers of opportunity, leadership, and governance, and to serve as a national resource and advocate for the municipal governments it represents.

NLC appreciates the opportunity to present a municipal perspective on the state of interoperable communications. Let me begin with a brief summary of NLC's initial recommendations to Congress:

(1) Elevate the visibility of the SAFECOM program for interoperable communications within the Department of Homeland Security.

(2) Build on the "spine" of existing communications networks to promote enhanced regional public safety and disaster response capabilities.

(3) Provide state and local governments with federal funding flexibility.

(4) Accelerate efforts necessary to implement the "date certain" return of analog spectrum required to improve public safety communications.

These recommendations represent a starting point for action. Action is necessary now because no one knows when or where the next natural or man-made crisis may strike that demands a rapid response and seamless communications among and between first responders and others engaged in public safety. For many communities and regions across the country, the challenge of interoperable communications represents an immediate threat to the viability of their public safety operations.

In my hometown of Beaverton, which is part of the greater Portland metropolitan area, we approach interoperable public safety communications from a regional perspective because public safety is an issue that does not respect artificial political or geographic boundaries.

I. Interoperability in Beaverton, Oregon

I have served as Chair of the Portland-area Regional Emergency Management Group (REMG) since 1993. This is a voluntary group formed through intergovernmental agreement between special districts, city, county and regional agencies in the five-county, bi-state Portland/Vancouver Metropolitan area. It includes the American Red Cross and steady participation from utility providers and local and global businesses such as Portland General Electric, Northwest Natural Gas, Bonneville Power Administration, PacifiCorp, and Intel.

Subsequent to the formation of REMG, the Department of Homeland Security Urban Area Security Initiative (UASI) designated the Portland/Vancouver Metropolitan area as one of the key regions nationwide at risk from potential disasters—natural or man-made. The UASI funds provide resources for the equipment, planning, and training needs of these designated regions.

REMG is the vehicle by which the public and private sectors in the Portland/Vancouver region work together to organize, plan and define regional needs and develop common policies and procedures to follow in the event of a disaster. The group is dedicated to providing a long-term model for regional coordination and planning driven by operational necessity, not by financial incentives. The REMG consists of two committees:

- Technical Committee (REMTEC)—Comprised of emergency management professionals from the signatory agencies.
- Policy Advisory Committee (REMPAC)—Comprised of elected officials from all the signatory agencies.

The key initiatives for REMG include:

- Identification and publication of regional emergency transportation routes in cooperation with transportation officials from the region.
- Development of the Great Portland/Vancouver Area Emergency Alert System (EAS) Operation Plan in coordination with broadcasters across the region.
- Development of a regional disaster debris management plan in cooperation with "Metro," Portland's regional government, and local solid waste program managers.
- Voluntary agreement between local governments to address emergency management issues for the benefit of the entire region, regardless of resources or participation in the group.
- Staff deployment from participating agencies, without compensation, to work with the regional partners for the benefit of the entire region.
- Involvement of policy level representatives from each signatory agency who provide structure to the group and assist in developing sound policies and procedures for use in disaster situations.
- Emphasis on policy level coordination, resource management, and joint training and information management.

REMG works effectively because its signatory agencies believe in the value of a regional plan. A separate functional policy level allows technical experts such as emergency management professionals to focus solely on achievements at the field level. These officials also provide accountability and oversight for the group. REMG provides a place for business, government, and disaster relief organizations to have a voice and collaborate in disaster planning. REMG does face challenges including its ineligibility to receive federal grant funding directly, and its lack of statutory authority. However, a regional plan ensures the integration of all individual plans within a common plan.

There are many advantages to coordinated emergency response. First, it develops proactive partnerships between likely co-responders. A diverse group of partners provides the opportunity to capitalize on the strengths of each for policies and procedures, knowledge and funding. Second, it brings together from across our region a collective knowledge for the benefit of the entire region. This is more powerful than each entity working alone and in competition for available resources. Third, it re-

duces duplicate efforts, helps identify and allocate finite resources, maximizes resource utilization, and ensures communication of a consistent message to the public.

As stated in *"A Failure of Initiative," a final report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina:*
"The failure of initiative was also a failure of agility. Response plans at all levels of government lacked flexibility and adaptability. Inflexible procedure often delayed response. Officials at all levels seemed to be waiting for the disaster that fit their plans, rather than planning and building scalable capacities to meet whatever Mother Nature threw at them." *Executive Summary at 2* (February 15, 2006).

While direct funding for local projects helps day-to-day, mission-critical capabilities for any given agency, it does not always guarantee a benefit or ensure coordination when major incidents like large weather disasters or an earthquake involving multiple jurisdictions and disciplines strike. To remedy this situation, Congress should support mechanisms that encourage, streamline and improve coordinated planning on a regional level. There is a need to transcend traditional barriers associated with jurisdictional boundaries or "turf issues."

For instance, regional jurisdictions and disciplines must train together on the plans within the Incident Command System (ICS) environment. Our nation needs a multi-jurisdictional, multi-disciplinary approach to public safety planning inclusive of all levels of government and parties affected—urban and rural. The challenge for our national emergency preparedness system is to integrate local, state, and federal government resources and ensure that federal money provides incentives to develop integrated systems.

II. NLC Position on Interoperability

Since 1995, NLC has been a national leader in support of clearing radio spectrum for public safety use. This was the year when domestic terrorists bombed the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma. In the intervening years, our nation has experienced dramatic natural disasters such as Hurricanes Katrina and Rita, and terrorist attacks on the Pentagon and World Trade Centers. NLC's policy states that "[t]he federal government must allocate sufficient telecommunications spectrum to cities for public safety use in order to enhance inter-operable communications among public safety and service agencies, and to ensure the ability of local governments to meet their responsibilities for public safety and emergency services. *ational Municipal Policy at § 7.04 A. (2006).*

Last December 2005, NLC adopted a resolution during its annual governance meeting that re-affirmed its long-standing position that interference-free broadcast spectrum and reliable and interoperable wireless communications are essential to the public safety role of local officials. *NLC Resolution #2006–46.* The resolution expresses that "past federal public safety frequencies and channels have been scattered and inadequate, resulting in a fragmented public safety spectrum." *Id.* The federal government "must lead the efforts to resolve interoperability problems that affect emergency communications and data systems throughout the nation." *Id.*

Since the Oklahoma City bombing in 1995, NLC worked to ensure that city leaders have the resources and the best possible capabilities to prevent serious attacks in their communities and to respond when a catastrophic event occurs. In 1997, NLC coordinated with key Senate leaders and then-U.S. Attorney General Janet Reno to obtain new wireless telecommunications capacity exclusively for state and local public safety use. In addition, NLC supported a requirement in the *Balanced Budget Act of 1997* that the FCC reallocate 24 megahertz of spectrum in the upper portion of the 700 MHz band (channels 60–69) for public safety use.

In 1998, NLC co-authored with the Department of Justice a guidebook entitled, *Public Safety and Radio Spectrum Guide,* to help city leaders enhance their public safety communications capacity. The following year, NLC spotlighted the need for vigilant legislative and regulatory action to clear the radio spectrum for public safety communication needs. Oklahoma City Councilwoman Ann Simank, a member of NLC's Public Safety and Crime Prevention Steering Committee, described the chaotic scene of the bombing site in testimony before the House Government Reform Subcommittee on Oversight, Investigations, and Emergency Management:

"That morning we learned first-hand the extreme importance of interoperable voice communications. Under the best of circumstances, when terrorism or natural disasters strike, you are working in chaos. But when you can't communicate, your hands are tied."

Two years later, the events of September 11, 2001, and the shortcomings of public safety communication systems that day served as a deadly reminder of Councilwoman Simank's testimony. Our first responders must have timely information and resources to lead the way in emergency response. Unfortunately, because emergency responders do not share common broadcast frequencies, lives are at risk. The 9/11

Commission's Final Report specifically stated that the inability of these first responders to talk with each other and their commanders resulted in loss of life that day. The 9/11 Commission identified the need for more spectrum as *crucial* to assist police, firefighters, and emergency responders in communicating during an emergency such as a terrorist attack or a hurricane.

The radio spectrum is a finite, non-renewable natural resource owned by the people and managed by its elected officials. Having the capability to transmit vital information to different emergency response personnel among all levels of government without interference and delay is key to disaster preparedness and emergency response. Only the federal government can remedy the current availability shortage of broadcast spectrum for public safety needs across the nation.

III. Recommendations to Congress to Improve Interoperability

Whether at the local, county, regional, state, or federal level, as elected officials we have one common link. We generally represent the same constituents and they remind us of shortfalls when large disasters such as Hurricane Katrina befall us.

The challenge of integrating levels of service provision is daunting. I have helped guide regional cooperation among local officials for the last 13 years and it has taken skill and commitment to keep us on task. We began the REMG in 1993, but our work became even more focused after a major windstorm hit the Portland/Vancouver area in late 1995. Our collective response was weak with poor communication and cooperation between agencies and the utility providers. In post-event evaluations, we recognized that we failed in many ways and committed to improving communication, response and planning. All of this happened long before the tragic events of 9/11. We seek partnership and financial assistance from Congress to implement local and regional plans. Moving beyond our own boundaries to a collective response is desirable, but funding becomes the big obstacle at each turn.

I would recommend the following to strengthen the federal role in interoperable communications:

(1) *Elevate the Visibility of Project SAFECOM.*

NLC policy calls for the federal government to establish a comprehensive spectrum management master plan that includes input from all stakeholders, including local government. *National Municipal Policy at* § 7.04 C. Project SAFECOM at the Department of Homeland Security is a great example of a federal agency incorporating the input of local governments to improve interoperable communications plans and guidelines. Elevate the visibility of Project SAFECOM and its mission because interoperable communications capacity influences hometown security directly.

While we have built a functional and interoperable radio communication system in the Portland/Vancouver area, this is not the case on a national basis. The federal government should encourage regional planning for public safety communication needs and address the current shortage of spectrum channels with a long-term plan that ensures available broadcast channels to meet future public safety needs across the nation. If federal reallocation of radio spectrum forces a municipality to change radio frequencies, channels, or both to preserve its public safety and emergency communications services, then in consideration there should be prompt and fair compensation paid for transfer costs, such as new equipment and additional personnel and training.

(2) *Build on the "spine" of existing communications networks.*

NLC recommends that Congress encourage states to facilitate local and regional interoperable communications efforts that build on the "spine" of communications networks that promote enhanced public safety and disaster response capabilities across multiple jurisdictions and areas. The federal government should design programs that benefit first responders at the local level, but within a national scheme. Congress should support the construction and maintenance of emergency preparedness plans and communications infrastructure systems that operate not only within the internal system for day-to-day mission-critical tasks, but are also "interoperable" between disciplines when major emergencies escalate.

Related, the federal government should commit to link all emergency warning systems and supply all areas with appropriate equipment so that we leave no area unprotected. *National Municipal Policy* at § 6.02 E.2. (2006). Emergency alert systems should be used to ensure that any emergency declared by the President, homeland security, or through National Weather Services alerts are timely and accurate and provide direction on recommended protective measures local governments should take when the threat level is increased. Reimbursements to local governments for any costs associated with heightened alerts are necessary.

NLC urges the federal government to ensure that all areas of the country have access to modernized 911 technologies for emergency use. Currently, cities and

towns that do not have timely emergency response services usually have not implemented a 911 system or their systems are antiquated. NLC also urges the federal government, in particular the Department of Justice and the Federal Communications Commission, to continue its efforts to improve the wireless 911 or E–911 services by working in partnership with state and local land use authorities, public safety officials, and the telecommunications industry. In addition, the telecommunications industry must fully develop and fund wireless emergency locater services, tracking systems, and lead efforts to resolve interoperability problems that affect emergency communications systems throughout the nation. These efforts must continue to respect the premise of local autonomy, avoid burdensome mandates, and reflect the need for greater funding in underserved jurisdictions.

The federal government must also involve cities as it develops standards for the delivery of emergency information on cable systems. National Municipal Policy at § 7.04 A. (2006).

(3) *Funding Flexibility.*

NLC urges Congress to allow more flexibility in the use of federal public safety funds for upgraded technology communication systems and training. Many municipalities face great difficulty in purchasing necessary public safety equipment because of budget constraints or their inability to qualify for available funds. New duties placed on law enforcement related to homeland security have shrunk budgets further. NLC urges the federal government to assist all municipalities in advancing their public safety capabilities without imposing inflexible compliance guidelines.

Local governments are the first level of government to respond to most disasters and emergencies. The federal government should provide funding directly to local governments for homeland security, emergency preparedness, and response because we are the initial focal point of all disaster mitigation and recovery activities. The structure of federal and state technical and financial assistance should allow local officials maximum flexibility in meeting identified needs. Regarding the homeland security funding formula, NLC supports the federal government continuing to fund risk-based threats in highly populated and high-threat areas. NLC also supports a minimum level of funding for state grants sufficient to allow jurisdictions to prepare for possible terrorist-based threats, with flexibility to use the funds for dual-use (risk and all-hazards) pursuant to their state homeland security plans. *National Municipal Policy at* § 6.03 A. (2006).

(4) *Federal Commitment to "Date Certain" for Return of Analog Spectrum.*

While NLC acknowledges the political challenges that led to a "date certain" return of analog spectrum by February 19, 2009, NLC reminds Congress that more lives than necessary may be lost between now and then because of a lack of spectrum. No one should lose his or her life because public safety officials cannot communicate with one another. NLC urges Congress to lead the efforts to accelerate, if possible, efforts to resolve interoperability problems that affect emergency communications and data systems throughout the nation. Reliable and interoperable wireless communications are essential to public safety's mission to protect life and property.

* * *

Thank you for the opportunity to present the views of municipalities on the important work of building interoperable communications networks.

ATTACHMENT ONE
NLC RESOLUTION #2006–46
IN SUPPORT OF INTEROPERABLE PUBLIC SAFETY COMMUNICATIONS SYSTEMS AND FUNDING

WHEREAS, interference-free broadcast spectrum and reliable and interoperable wireless communications are essential to the public safety role of local officials;
WHEREAS, the federal government has a responsibility in providing adequate telecommunications spectrum to enhance interoperable communications among public safety and emergency services;
WHEREAS, past federal public safety frequencies and channels have been scattered and inadequate, resulting in a fragmented public safety spectrum;
WHEREAS, the federal government must provide funding to purchase the necessary equipment and training; and
WHEREAS, federal funding of interoperable public safety equipment continues not to meet the new needs and requirements of the post September 11th environment.
NOW, THEREFORE, BE IT RESOLVED that the federal government must lead the efforts to resolve interoperability problems that affect emergency communications and data systems throughout the nation;

BE IT FURTHER RESOLVED that the federal government must remedy the current shortage of broadcast spectrum availability for public safety needs across the nation;
BE IT FURTHER RESOLVED that the federal government must provide adequate funding for interoperable equipment to better facilitate coordinated and effective emergency response in cites and across jurisdictions; and
BE IT FURTHER RESOLVED that the National League of Cities (NLC) insist that Congress adhere to the December 31, 2006 compliance date for vacation of television channels currently blocking radio spectrum required for public safety radio communications systems.

Mr. REICHERT. Thank you, Mayor Drake.

The Chair recognizes Mr. Menchini.

STATEMENT OF HON. OGINO MENCHINI, COMMISSIONER, DEPARTMENT OF INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS, NEW YORK CITY

Mr. MENCHINI. Thank you, Mr. Chairman, and thank you, distinguished members of the subcommittee.

Good afternoon. My name is Gino Menchini. I am getting over a cold, so please bear with my voice. But I am commissioner of the New York City Department of Information Technology and Telecommunications, and the city's chief information officer. Accompanying me today is Inspector Charles Dowd, commanding officer of the New York City Police Department's Communications Division.

I am privileged to have the opportunity to testify before you today about public safety communications in the city of New York, to describe the interoperable systems we have put into place and to outline the city's future needs.

Allow me to begin by saying that one of the primary challenges in designing interoperable radio systems is anticipating the many different circumstances in which interoperable communications will be required. This type of contingency planning is fundamental because, contrary to popular belief, interoperability cannot be achieved by simply putting thousands of emergency responders onto the same radio channel.

I see you are nodding because I think Los Angeles has a similar situation that New York City does.

The shortcomings of such an approach mirror limitations associated with telecom voice traffic, generally. For example, just as it would create havoc to have thousands of participants on a single telephone conference bridge, so too would essential radio communications become jumbled and lost, with too many responders talking at the same time, on the same channel.

To do their jobs effectively and safely emergency responders must have specific channels dedicated to those personnel participating in particular operations. These personnel must not be required to contend with the traffic of other users communicating about something other than the mission at hand.

Some believe that an alternative means of achieving interoperability would be for responders to scan through their radio channels in search of information that might be useful to them. This approach overlooks the fact that emergency responders generally must remain on their primary incident radio channel or else risk losing critical messages related to command, control and coordination.

As I said, achieving interoperability solutions really does depend on our ability to specifically anticipate the types of situations in which interoperable communications will be required. Since September 11, the city has focused on defining these interoperability requirements and on tailoring interoperability initiatives to address them.

In regard to first responder interoperability, the city has made the determination that the optimal approach is to bring all users onto a common UHF frequency band so that interoperability can be achieved among police officers, firefighters and emergency medical technicians when the circumstances dictate that particular users from these forces must communicate with each other.

In this regard, in 2004, the FCC permanently allocated TV broadcast channel 16 for the use of public safety communications by multiple New York City agencies, including the police departments and fire departments, emergency medical services and the Office of Emergency Management, as well as neighboring counties. The channel 16 frequency band is used in various situations that require interoperable communications. These range from on-scene mission-specific interoperable communications between walkie-talkies, to communications on a borough or citywide basis among officials from different agencies, to communications on a regional basis.

In regard to secondary responder interoperability, I want to outline how we have addressed these requirements for interoperable communications during major incidents. The city has implemented specialized talk groups on our citywide 800 MHz system for 56 state, city and regional agencies; 78 hospitals and healthcare facilities; and the commissioners of 44 city agencies.

For multi-jurisdictional interoperability, in the aftermath of September 11, the city has established a regional Interoperability Communications Committee, known as the ICC. The ICC meets regularly to evaluate the current state of interoperable communications and to develop strategies for improving interoperability.

Finally, the city has deployed several TRP–1000 radio interoperability systems to provide interoperability during incidents that require communications among city, state, regional and federal organizations using different radios and different frequency types. The ICC has established protocols for the deployment of TRP–1000s to support the tactical communications of these multijurisdictional agencies at a scene.

I should emphasize that achieving interoperability is an ongoing process, rather than an end state that we can never perfectly achieve that interoperability, and it must be dynamic and meet the changing requirements and changing needs of our first responders.

Obtaining adequate funding is, however, critical for these endeavors. I will describe briefly some of the interoperability projects the city is currently pursuing.

For tactical interoperability communications plan, the city is in the process of finalizing its tactical interoperability communications plan, which will be submitted to the Department of Homeland Security by May 1. This plan will document what interoperable communications resources are available within our urban area and who

controls each resource, as well as the rules and operational procedures for the appropriate use of each interoperable resource.

The creation of this plan is a requirement of the Department of Homeland Security Office of Grants and Training 2005 Urban Area Security Initiative Grant Program. The city is fully compliant with the Department's requirements.

I am going to go over my time here, if that is okay. Is it? Thanks. I hope this is of value. And as a New Yorker, I can speak much quicker, but you may not be able to understand it.

On the implementation of 700 MHz, the city certainly appreciates the establishment of a firm date for transfer of the 700 MHz spectrum, as well as the congressional allocation of $1 billion for interoperability contained in the budget reconciliation bill recently signed by the President. Clearly, however, $1 billion when dispersed throughout the nation is not sufficient to fund optimal use of the 700 MHz system, and we would urge you to consider expanding funding for this initiative.

As you know, this spectrum was allocated to public safety with three main objectives: One, to provide much needed additional public safety voice channels, and, two, to improve regional Interoperability, as well as allow for transmission of wideband data.

In regards to wideband data, the city is moving aggressively to deploy a state-of-the-art interoperable citywide mobile broadband data network, which will provide emergency responders with data access to large files, including maps, building layouts and massive federal and state anti-crime and anti-terrorism databases, as well as mug shots of terrorists and be able to have video-on-demand coming to and from scenes. These networks will provide for downloads of full-motion video at emergency scenes and continuous biological, chemical, nuclear and radiological monitoring.

The transmission capability of this network will be the first of its kind and will literally transform the way in which officials respond to emergencies. Given the substantial public safety and national security components of the project, the city is pursuing federal funding to offset its costs, which will be several hundred million dollars.

With regard to funding, I would like to recommend that Congress consider establishing funds specifically for local governments. Ultimately, local governments are in the best position to determine their public safety needs and establish local first responder programs that can provide for interoperability based on the specific needs of the given area.

I would also like to emphasize that some of the key criteria that should be applied in the allocation of funds should be level of risk, population concentration and consequences associated with damage to critical economic and physical infrastructure.

Let me close by thanking you again for the opportunity to provide you with the overview of what the city has been doing to improve interoperability and our funding needs for these endeavors. I would be pleased to answer any questions that you may have.

[The statement of Mr. Menchini follows:]

PREPARED STATEMENT OF HON. GINO P. MENCHINI

WEDNESDAY, MARCH 1,2006

Good afternoon. I am Gino Menchini, Commissioner of New York City's Department of Information Technology and Telecommunications, and the City's Chief Information Officer. Accompanying me today is Inspector Charles Dowd, Commanding Officer of the New York City Police Department's Communications Division. I am privileged to have the opportunity to testify before you today about public safety communications in the City of New York; to describe the interoperable systems we have put into place; and to outline the City's future needs.

Allow me to begin by saying that one of the primary challenges in designing interoperable radio systems is anticipating the many different circumstances in which interoperable communications will be required. However, this type of contingency planning is fundamental because, contrary to popular belief, interoperability cannot be achieved by simply putting thousands of emergency responders onto the same radio channel.

The shortcomings of such an approach mirror limitations associated with telecom voice traffic, generally. For example, just as it would create havoc to have thousands of participants on a single telephone conference bridge, so too would essential radio communications become jumbled and lost, with too many responders talking at the same time, on the same channel.

To do their jobs effectively—and safely—emergency responders must have specific channels dedicated to those personnel participating in particular operations. These personnel must not be required to contend with the traffic of other users communicating about something other than the mission at hand.

Some believe that an alternative means of achieving interoperability would be for responders to scan through their radio channels in search of information that might be useful to them. This approach overlooks the fact that emergency responders generally must remain on their primary incident radio channel, or else risk losing critical messages related to command, control, and coordination.

As I said, achieving interoperability solutions really does depend on our ability to specifically anticipate the types of situations in which interoperable communications will be required. Since 9/11, the City has focused on defining these "interoperability requirements," and on tailoring interoperability initiatives to address them.

First Responder Interoperability

With respect to first responders, the City has made the determination that the optimal approach is to bring all users onto a common UHF frequency band; so that interoperability can be achieved among police officers, firefighters, and emergency medical technicians when the circumstances dictate that particular users from those forces must communicate with each other.

In this regard, in 2004, the FCC permanently allocated TV broadcast Channel 16 for the use of public safety communications by multiple City agencies, including the Police and Fire Departments, emergency medical services, and the Office of Emergency Management, as well as neighboring counties. The Channel 16 frequency band is used in various situations that require interoperable communications. These range from on-scene mission specific interoperable communications between walkie-talkies, to communications on a borough or City-wide basis among officials from different agencies, to communications on a regional basis.

Secondary Responder Interoperability

Next, I would like to outline how we have addressed secondary responder requirements for interoperable communications during major incidents. The City has implemented specialized talk groups on our Citywide 800 MHz system for 56 City, State, and regional agencies; 78 hospitals and healthcare facilities; and the commissioners of 44 City agencies.

Multi-Jurisdictional Interoperability

Let me now turn to multi-jurisdictional interoperability. In the aftermath of 9/11, the City established a regional Interoperability Communications Committee (known as the "ICC"). The ICC meets regularly to evaluate the current state of interoperable communications and to develop strategies for improving interoperability.

Finally, the City has deployed several TRP-1000 radio interconnection systems to provide interoperability during incidents that require communications among multiple City, State, regional, and Federal organizations using different radios and different frequencies. The ICC has established protocols for the deployment of TRP-1000s to support the tactical communications of these multi-jurisdictional agencies at a scene.

Other Interoperability Initiatives

I should emphasize that achieving interoperability is an ongoing process, rather than an "end state" that can ever be perfectly achieved. Obtaining adequate funding is, however, critical for these endeavors. I will describe below some of the interoperability projects the City is currently pursuing.

Tactical Interoperability Communications Plan

The City is in the process of finalizing its Tactical Interoperability Communications Plan which will be submitted to the Department of Homeland Security by May 1, 2006. This plan will document what interoperable communications resources are available within our urban area, and who controls each resource, as well as the rules and operational procedures for the appropriate use of each interoperable resource. The creation of this plan is a requirement of the Department of Homeland Security Office of Grants and Training 2005 Urban Area Security Initiative grant program. The City is fully compliant with the Department's requirements.

Implementation of 700 MHz

The City certainly appreciates the establishment of a firm date for transfer of the 700 MHz spectrum, as well as the Congressional allocation of $1 billion for interoperability contained in the Budget Reconciliation Bill recently signed by the President. Clearly, however, $1 billion when dispersed throughout the nation is not sufficient to fund optimal use of the 700 MHz spectrum, and we would urge you to consider expanding funding for this initiative. As you know, this spectrum was allocated to public safety with three main objectives: (1) to provide much needed additional public safety voice channels; (2) to improve regional interoperability; and (3) to allow for transmission of wideband data.

Citywide Wireless Network

The City is moving aggressively to deploy a state-of-the-art interoperable Citywide mobile broadband data network, which will provide emergency responders with data access to large file transfers, including maps, building layouts, and massive Federal and state anti-crime and anti-terrorism databases. These networks will provide for downloads of full-motion video at emergency scenes, and continuous biological, chemical, nuclear, and radiological monitoring.

The transmission capability of this network will be the first of its kind and will literally transform the way in which officials respond to emergencies. Given the substantial public safety and national security components of the project, the City is pursuing federal funding to offset its costs, which will be several hundred million dollars.

With regard to funding, I would like to recommend that Congress consider establishing funds specifically for local governments. Ultimately, local governments are in the best position to determine their public safety needs and establish local first responder programs that can provide for interoperability based on the specific needs of the given area. I would also emphasize that some of the key criteria that should be applied in the allocation of funds should be level of risk, population concentration, and consequences associated with damage to critical economic and physical infrastructure.

Let me close by thanking you again for the opportunity to provide you with this overview of what the City has been doing to improve interoperability and our funding needs for these endeavors. I would be pleased to answer any questions you may have.

Mr. REICHERT. Thank you, Mr. Menchini.

Chief Werner?

STATEMENT OF CHARLES WERNER, FIRE CHIEF, CHARLOTTESVILLE FIRE DEPARTMENT, COMMONWEALTH OF VIRGINIA

Chief WERNER. Mr. Chairman, distinguished members of the committee, thank you very much, and let me commend you on your bipartisan commitment to working toward interoperability for us. We appreciate that.

My name is Charles WERNER. I am the fire chief for the city of Charlottesville, Virginia, and I have been in the fire rescue service for over 30 years.

In addition to that, I serve on the International Association of Fire Chiefs Communications Committee. I am the Virginia fire chiefs interoperability technology chair, and I serve on the State Interoperability Executive Committee and was the first and, fortunately now I can say, past chair of that Interoperability Executive Committee.

What we get to now is understanding, as we have all said—and I am not going to get into too much detail—but citizens rely on us to have the communications that we need. They expect it, and the for the most part they thought we had it. For many of us, as Mr. Chairman has already mentioned, for over 30 years, there has been a problem with this issue of operability and interoperability. It is nothing new. We have just had a highlighted focus that hopefully will move us to getting that taken care of.

Radio operability is critical for public safety agencies to maintain the communications capability to protect safety of life and property, and in cases of larger, more complex incidents, interoperability becomes important in order for us to maintain the continuity of command and control. And you are going to hear that repeatedly.

Interoperability has been an ongoing issue for public safety for decades and reinforced after these major catastrophes.

Since 9/11, the need for public safety communications interoperability has increased as law enforcement, fire, EMS and emergency managers are asked to assume greater roles in homeland security.

Today, I will speak to you from three vantage points. First, I will give you an overview from the 10,000-foot view, as I review Virginia's efforts from the statewide Interoperability Executive Committee's perspective. Second, I will provide you a view from ground level where I serve as a regional interoperability project manager for the city of Charlottesville, the county of Albemarle and the University of Virginia. And, last, I will express my experiences and observations at the national level, as I serve on SAFECOM's Executive Committee as one of public safety's practitioner members.

In Virginia, it is interesting, because the methodology that we ended up choosing was what SAFECOM had already done. As a member of the SAFECOM Executive Committee, I observed the development and the involvement of practitioners to understand that really to get a firm understanding of what we need and where we need to go, you need to involve the people who know how to get there and what they need.

And that is just what we did. We mirrored SAFECOM's philosophy and the methodology, which is now the model that is set up on the SAFECOM Web site that allows you to pull that stripped Virginia pieces to a methodology that can be emulated by any state that desires.

What is really interesting and important about this process is that not only is it practitioner-driven but it is driven by people processes, getting the people in the positions that are responding to these emergencies together, across disciplines—fire, police, EMS, emergency managers—together to talk about what we need.

And what we found out was something unique: We are a lot more alike than we are different. And, operationally, when it comes to a situation that we have to deal with, together, collectively, it is going to take us to solve it.

The state methodology is broken down in 10 phases.

Phase one—and please note, this is the most important point here—is to establish key relationships and funding. The relationships are number one, because without the relationships then working together collectively, we are not coming up with a solution that is going to be universal. And developing those relationships will be key in everything else that happens in the rest of this process.

There is a very significant thing I would like to share as an experience. There is a very different thing that happens when you work with someone you do not know and when you work with a friend. When you call an ask for a resource from a friend, that friend says, "When and where do you want it." When you do not have that relationship, the question gets into, "What do you need it for, why do you need it, who gave you the authority to ask me for it?" This is a key point.

Phase two is, gather the information, what is it that we need. Then from that information create a project plan and a road map. I think that many of us have heard that without road map any road will lead you to where you want to go. And if we do not have that road map, we are all going in different directions.

Phase four is, identify roles and responsibilities.

Phase five, recruit focus group participants. Make sure that you have all the stakeholders involved, and that includes appointed and elected officials, because we ca not move this process forward without an understanding and support.

Conduct focus group interviews to find out more specifically what is needed.

Phase seven, analyze the data and prepare for strategic planning sessions. Bring the people together, now talk about it. And what we found in these sessions was really interesting. There were efforts underway in regions that people knew nothing about, that suddenly there were opportunities that we could take advantage of that we did not even know about before.

Nine, develop statewide communications interoperability strategic plan.

And then phase 10 is, guidelines for the first 90 days to launch what you have started. What we have seen too many times is that we do not follow through once we have the plan.

In Virginia's situation, the outcome yielded the formation of the Interoperability Executive Committee, an advisory group, the hiring of a full-time interoperability coordinator, implemented a Supportive Program Management Office, conducted two statewide interoperability conferences, developed, implemented and updated the Statewide Interoperability Strategic Plan, legislated the plan would be updated annually and that by 2015 anything grant oriented would meet the requirements or the goals of that particular plan.

Virginia's success would not have been possible if it were not for Governor Warner and his administration. Again, this is about bipartisanship and about everybody working together. And I would also be remiss if I did not mention George Foresman who is now our under secretary of emergency preparedness, who, too, was right side by side making these things happen.

And, last, and importantly, on this particular issue at the state level, it is the funding. The funding was key to the element of getting Virginia launched and making things happen.

As far as locally, a national demonstration project in Charlottesville is proof again that the SAFECOM model works now at the ground level where the boots are on the ground, where the rubber meets the road.

And I have to say this, by the city manager, me being here today, is that in 2004, Charlottesville was chosen as the number one city, and it is largely because probably of our cooperative spirit, and this regional effort that we have done as the city of Charlottesville, the county of Albemarle and the University of Virginia, with a land mass of 744 square miles of both flat and mountainous terrains.

The University of Virginia increased its student population, staff, and in addition to that, we have some very national treasures: Thomas Jefferson's home, Monticello, and James Monroe's home, Ashlawn.

In 2003, a $6 million grant was given to the city of Charlottesville, the county of Albemarle and the University of Virginia because of the projects, and I want to go through it very quickly to tell you the scope. And I am going to go through some of the references here, not to endorse any particular project but just to give you the scope of what was involved.

First, we developed a parallel and secondary logistical network for the use of Nextel push-to-talk technology for the sheer reason that the push-to-talk technology here is not dependent on the public telephone switch.

In the process of implementing a robust Motorola 800 megahertz digital analog public radio system that will bring together all public safety agencies in our region, including the jails, the airports, everything that has to do with public safety and will support NIMS and the National Response Plan.

We are in the process now of creating a console integration between the Nextel parallel network and our public safety network, which allows us to bring in non-public safety agencies in an affordable way to create interoperability and a whole community approach. Because what we have learned through this process is that public safety alone cannot handle the situations, especially of extreme magnitude, that are necessary.

And we are in the process of putting in place a M–A/COM mobile data system that will support us on the data side.

Mr. REICHERT. Chief, can you do this in 1 minutes and 20 seconds?

Chief WERNER. One minute.

Mr. REICHERT. Okay.

Chief WERNER. Tactically, we have an incident command radio interface that we put in place and Edge Access to do satellite communications. And that equipment was sent to Hancock, Mississippi and was in operation there for 20 days.

Let me just get to the 30,000-foot view really quick. What we have seen is SAFECOM is the agency which focuses on the federal oversight of interoperability, and what I envision here is that we need to make sure that it has made impacts and that it needs to be made strong and kept strong.

Standards are important, but be careful when you do standards, because it does not necessarily mean it is going to cover all the bases. An example, a smaller public safety agency that does not have a trunked radio system does not need to buy a $4,000 P25 radio when a $500 analog radio would suffice.

And, last, operability needs to be handled first to make sure the system works, because interoperability does not matter after that. And we need to commit to interoperability in the long term. This is not a short-term process.

And, finally, recognize that full interoperability and all the critical live-saving capabilities it offers is a long-term mission. Do not sacrifice the long-term goal of full interoperability by focusing only on the near-term problem.

And one last thing I want to leave you graphically. I brought today one of many gateways that are available. If I walked up and handed this to you and said, "Here, you have interoperability," you would not have it. If one of these or any device similar was given to every city in the country, the thought process is that interoperability happens. But I want to leave it on the thought of it is about a people process. It is about the governance and the cooperation between people that we must continue to work on. And, again, SAFECOM is that vision to help us move in that direction.

Thank you.

[The statement of Chief Werner follows:]

PREPARED STATEMENT OF CHARLES L. WERNER

WEDNESDAY, MARCH 1, 2006

DEVELOPING A SPECIFIC INTEROPERABLE COMMUNICATIONS STRATEGY IS PARAMOUNT TO SUCCESS

Thank you, Mr. Chairman, and members of the Committee for the opportunity to appear before you today.

My name is Charles Werner and I am the Fire Chief for the City of Charlottesville, Virginia and have served in the fire-rescue service for over 30 years.

I serve on the Communications Committee of the International Association of Fire Chiefs (IAFC). I also serve as the Virginia Fire Chiefs Technology/Interoperability Chair and on the Virginia Statewide Interoperability Executive Committee (VA SIEC—past Chair).

Citizens rely upon their local and state police agencies, sheriffs' offices, fire departments and emergency medical services to come to their assistance wherever and whenever needed, whether it is crime in progress, a civil disturbance, a building fire, a forest fire, an automobile accident, a health emergency, a natural disaster, or, as we learned on 9/11, a terrorist attack. Citizens assume that those first responders will get the call and will have the communications tools they need to address emergencies quickly and efficiently.

Radio operability is critical for public safety agencies to maintain the communications capability that we need to protect the safety of life and property. In cases of larger and more complex incidents interoperability becomes very important in order to maintain the continuity of command and control. Interoperability has been an ongoing public safety issue for decades and reinforced after major catastrophes across the United States.

Since 9/11, the need for public safety communications interoperability has increased as law enforcement, fire, EMS are being asked to assume greater roles in roles of homeland security.

Today, I will speak to you from three different vantage points. First I will give an overview from the 10,000 foot view by reviewing Virginia's efforts and outcomes. Second, I will provide you a view from ground level where I serve as the regional interoperability project manager for the City of Charlottesville, County of Albemarle and the University of Virginia. Last, I will express my experiences and observations

at the national level as I serve on SAFECOM's Executive Committee as one of its public safety practitioner members.

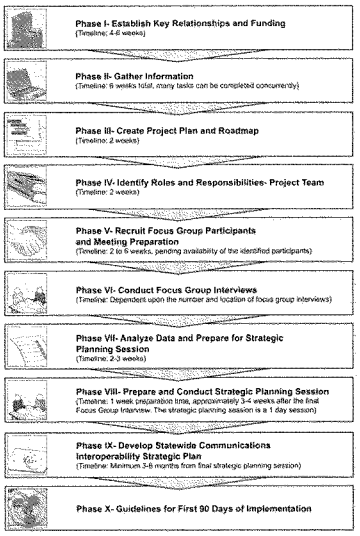
Virginia's Interoperability Efforts—"10,000 foot aerial view"

I have been specifically asked to explain about Virginia's methodology for developing a statewide interoperable strategic plan. Having served as Virginia's SIEC Chair during the majority of this process I am pleased to share what has been a very positive and proactive process.

The Virginia methodology for addressing interoperability at the state level mirrored the process developed by Office of Interoperability/SAFECOM. SAFECOM worked with Virginia to customize the methodology and was designed to be an effective tool to help local governments and states to improve public safety communications across disciplines and jurisdictions. Virginia's efforts resulted in a comprehensive plan that addresses the interoperability needs and challenges of Virginia's public safety community as identified by Virginia's public safety practitioners. The key is that the initiatives are public safety practitioner (boots on the ground) driven at the state and federal levels.

Virginia's Statewide Communications Interoperability Planning (SCIP) methodology has now been institutionalized as a model that can be accessed from the Internet (*http://www.safecomprogram.gov/SAFECOM/library/interoperabilitycasestudies/1223—statewidecommunications.htm*).

The SCIP methodology is broken down into ten essential planning phases that local government and states can use to create their own communications plan.



The process has yielded the following positive outcomes:

- Formation of Virginia's SIEC
- Formation of a supporting Advisory Group
- Hiring of a full time Interoperability Coordinator
- Implemented a supportive program management office
- Conducted two statewide interoperability conferences
- Developed, implemented and updated the Statewide Interoperability Strategic Plan
- Legislated that the Statewide Interoperability Plan would be updated annually
- Legislated that by 2015 grant funding would only be awarded to submissions that meet the goals of the plan
- A better understanding of what efforts were underway and ways to maximize them

Virginia's success in the area of interoperable communications would not have been possible if it weren't for the leadership and support of Virginia Governor Mark Warner and his administration. I would also be remiss if I did not acknowledge that much of this work was achieved alongside a very supportive cast member who now serves as our Under Secretary of Emergency Preparedness, George Foresman. Federal grant funding must be also noted as a key catalyst to those successes at the state and local levels.

Please carefully note that the successes in Virginia have been the result of the "people processes" and that technology only supports what people-in this case our local and state elected and appointed officials – have agreed to.

A National Demonstration Project:
Charlottesville-Albemarle-University of Virginia—"a ground level view"

The Charlottesville region is living proof that the Virginia (SAFECOM) model works. Chosen as the #1 City in America in 2004, this region includes the City of Charlottesville, County of Albemarle and the University of Virginia with a geographic land mass of approximately 744 square miles and includes both flat and mountainous terrain.

The University of Virginia (UVA) also adds the element of a university town with a sizeable student, faculty and staff population.

In addition to UVA, the region is home to other national treasures such as Thomas Jefferson's home, *Monticello* and James Monroe's home, *Ashlawn.*

In 2003, the region developed a national demonstration project that was submitted and awarded one of the few $6M FEMA Interoperable Communications Equipment grants. This project is governed by all three jurisdictions and public safety practitioners of every discipline (Law Enforcement, Fire, EMS, and Emergency Management).

An overview of what the region has done to create a robust, redundant and resilient interoperable system is as follows:

- Developed a parallel and secondary public safety communications network for logistical communications using Nextel's PTT (because Nextel's iDEN network is the only PTT or walkie-talkie service that does not rely on the public telephone switch).
- In the process of implementing a robust Motorola 800 MHz digital/analog public safety mission critical radio system which provides communications to every public safety agency in the region (20+ agencies). This will support the National Incident Management System (NIMS).
- In the process of implementing console integration between the Nextel iDEN network and the Motorola 800 MHz radio system to allow communication between Nextel talk groups and Motorola talk groups. This enables us to reach out to non public safety agencies to create an affordable way to establish a "Whole Community Approach" and bring in other agencies such as public works, health departments, schools and more.
- In the process of implementing a M–A/COM Mobile Data System that will serve all public safety agencies in the region to provide information such as law enforcement vehicle and criminal wants and warrants, building floor plans, emergency operations plans, etc.
- In addition to fixed infrastructure, this project also addresses tactical interoperability at an incident site beyond the normal day to day operations which meets the RAPIDCOM recommendations (to achieve incident interoperability within one hour of the incident) and supports the communications with the federal agencies as outlined in the National Response Plan (NRP). This tactical equipment was chosen because of its effectiveness, simplicity and price:
- Incident Commander's Radio Interface (ICRI)—tested and listed by several DoD evaluations. It is a true plug and play technology and is EASY.
- Edge Access self deploying Satellite—Voice over IP (VoIP) which also establishes satellite telephone service, an internet connection and establishes a quarter mile hotspot which can be set up in a matter of 5 minutes or less by simply turning on and pushing one button. THIS IS IN MY VEHICLE TODAY AND I WOULD BE GLAD TO DEMONSTRATE IT ANYTIME.

NOTE: CHARLOTTESVILLE FIRE DEPARTMENT's UNIT WITH THIS *TACTICAL EQUIPMENT RESPONDED TO AND WAS USED IN HANCOCK, MS* FOLLOWING HURRICANE KATRINA.

- In the area of situational awareness, the region has implemented WebEOC (same as the National Capital Region—Virginia, Maryland, District of Columbia) to share information between jurisdictions and disciplines.
- In the process of implementing DMIS (Disaster Management Interoperability Software). This is one of the E–Gov Disaster Management tools.
- In the process of implementing the Emergency Email Wireless Network to serve as interoperable communications with the public through email and other wireless devices.

SAFECOM's Efforts—"a 30,000 foot aerial view"

As one of the public safety practitioners that serve on the SAFECOM Executive Committee that has been directly involved at both the state and local level I would like to share the following observations:

1. SAFECOM is having a real impact and is a genuinely practitioner driven program. It is the primary federal focus on interoperability and needs to be made and kept strong.

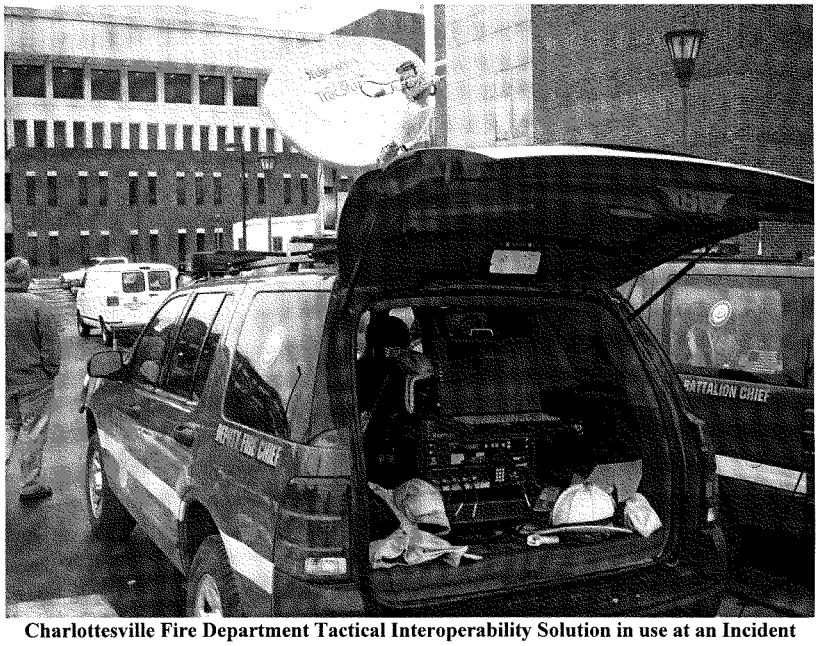
2. Standards are very important, but be cautious about requiring a particular standard to meet all occasions. For example, a smaller public safety agency that does not have a trunked radio system does not need to be buying $4,000 P25 radios when $500 analog radios would suffice. Make sure that standards are robust and can actually meet practitioner needs before requiring them.

3. Most of achieving near term interoperability is a matter of two things:

a. Build an effective "operable" system, first, then

b. Commit to interoperability because at the end of the day, achieving a reasonable level of emergency interoperability requires a willingness to cooperate among and between agencies and jurisdictions more than it requires a particular technology.

4. Finally, recognize that full interoperability, and all the critical life saving capabilities it offers, is a long term mission. Don't sacrifice the long term goal of full interoperability by focusing only on the near term problem.



Charlottesville Fire Department Tactical Interoperability Solution in use at an Incident

Contact Information:
Charles L. Werner● Fire Chief - Charlottesville Fire Dept. ●203 Ridge Street, Charlottesville, VA 22902 ● Telephone (434) 970-3240 ● E-Mail wernerc@charlottesville.org

Mr. REICHERT. Thank you, Chief.
Mr. Proctor?

STATEMENT OF STEVE PROCTOR, EXECUTIVE DIRECTOR, UTAH COMMUNICATIONS AGENCY NETWORK, (USCAN)

Mr. PROCTOR. Thank you, Mr. Chairman and members of the committee, for the opportunity to speak before you today.

My name is Steve Proctor. I am the executive director of the Utah Communications Agency Network, and I am also a representative of APCO, the largest public safety communication organization in the country, with about 17,000 members.

I personally have 35 years of experience in this field, beginning as an emergency dispatcher during my college training. I have also been privileged to serve on many national committees, FCC advisory committees and currently sit on the SAFECOM Executive Committee.

UCAN is a quasi-state agency that was established by our legislature for the sheer purpose of developing a radio system and serving currently 120 separate entities of government—state, local and federal. The system currently supports 15,000 users. It is governed by a board of directors made up of those users who set the rates, establish the budget, determine the direction and provide for the level of coverage.

One of our directors said it best: "We pay for the privilege of governing ourselves." And that is one of the key successes of this agency.

Our system in Utah experienced the acid test, providing interoperable communications during the 2002 Winter Olympic games. Not only were we responsible for supporting public safety, but we supported all the Salt Lake Organizing Committee events at each and every venue. During those 17 days, our system processed 10.5 million radio calls. That is about 400,000 calls per day.

We are here to talk about interoperability. The experience I described above with reference to UCAN did not come about magically. It took 6 long years of political compromise, negotiations and wrangling before the equipment order was ever placed. I hope as I briefly tell you how we got here some of these principles will aid you in determining where we take this public safety community nationally toward this sometimes elusive goal of being able to communicate with each other.

The first thing we did was identify the common pain that we all had together and that brought together all the stakeholders. We had a convener of stature, in this case our governor, who brought us all together, put us in a room and said, "Figure this out. Figure it out now."

A committed leader was appointed to broker the effort and to make sure that we directed—am I to stop or go ahead? Keep going? A committed leader was appointed to broker the effort and keep everybody focused on achieving results. There was a set of clearly defined purposes with predictable management and maintenance processes established. And all this was memorialized in a piece of legislation passed by our legislature establishing the agency.

After all those issues went through the process, then we talked about the money and how we were going to fund this effort and began to order the equipment.

So what does all this have to do with the committee? It has been said that during times of emergency, people expect government or at all levels to provide appropriate response to mitigate disasters, save lives, protect, support and help the needy and care for the injured. A major tool in providing that response is a communications system with reliable and dependable capabilities and capacity. There is simply no room for error.

The citizens we serve today expect in this world of miraculous technology that this is what will take place, and, sadly to say, that is not what takes place.

Why is that so? The public safety market is so limited in demand with a focused product line, that the equipment is costly to procure, maintain, upgrade and install. Most public safety radio systems are designed to last for 10 years, with many of them having to last for over 30 years. The system we replaced was 40 years old. Because of the limited market presence, the cost of individual units and equipment is very, very high.

There is a high degree of resistance from public safety entities supported by age-old political barriers that create roadblocks in motivating agencies to work together and share systems across city, county, state and federal lines. This is because there is a presumed loss of control.

So what can this committee do to assist the public safety entities and agencies across this country to achieve this interoperable goal? First of all, take a leadership role and support the SAFECOM program. This program is DHS' effort to promote interoperability. They cannot do it without proper staff, funding, direction and mission. With appropriate resources, SAFECOM can and should staff up with state and local experienced personnel who have a background in communications to assist them in this process. In many instances, this has been done by their Executive Committee made up of state and local members.

That federal government should tie future federal funding to performance measures, give priority attention to multi-agency, multi-disciplined projects with long-term goals and reasonable chances of success. The government should reward innovative projects and highlight them at association events, such as the police, fire chiefs and communications conventions, sending this message that funding will be tied to cooperative efforts.

Congress should establish long-term sustainable funding to support the public safety effort. This problem is not going to go away with one-time funding. It is going to take continued funding over a numbers of years period. Congress should push and sustain and provide funding to motivate the standards effort. As my distinguished colleagues have said before, the standards effort is what will allow manufacturers to build to a set of standards and have systems that will integrate with one another; therefore, driving down the cost.

I am quite sure, as you have already listened to many of these points many times; however, in actuality, they are the keys to success. While they are an important part of the process, this problem

will not go away with simply providing more frequencies and more money. What is required is true leadership, vision, bringing together all the players and resources to make better operability and interoperability possible.

Thank you. I would be happy to take any questions.

[The statement of Mr. Proctor follows:]

PREPARED STATEMENT OF STEVEN H. PROCTOR

WEDNESDAY, MARCH 1, 2006

Good Afternoon. Thank you Mr. Chairman and members of the committee for the opportunity to speak before you today.

My name is Steven Proctor. I am the Executive Director of the Utah Communications Agency Network (UCAN). I appear to today with the support of the Association of Public-Safety Communications Officials (APCO), the nation's oldest and largest public safety communication organization. I personally have 35 years of service in this field, beginning as a public safety dispatcher during my college training, and serving in various positions to my current position. I have also been active on the national level. I am a past-president of APCO, served on several FCC advisory committees, and currently sit on the SAFECOM Program Executive Committee.

UCAN is a quasi-state agency set up by the Legislature for the purpose of establishing a statewide public safety communications network. We operate a public safety communications system within the borders of Utah serving 120 separate state, local and federal government agencies. The system supports 15,000 users. A board of directors made up of our users manages the system. That board represents the user base in making decision concerning system implementation, growth, maintenance, and expansion. They also set the budget, determine the rates, and contribute towards the system growth and enhancement. One of our directors said it best: "we pay for the privilege of governing ourselves". That is one of the keys to success of this agency.

Our system, in Utah, has experienced the acid test of providing interoperable communications. That came four years ago when we supported the 2002 Winter Olympic games. Not only were we responsible for public safety radio traffic; we also supported the communications requirements of the Olympic organizing committee managing the venue events. During the events, our system processed 10.5 million requests to talk, supporting just under 16,000 radios. There were no major system failures, network traffic issues or inability to communicate.

We are here to talk about interoperability. The experience I describe briefly above did not come without a focused effort. It took six years of hard work, political compromise, negotiations and wrangling before the system equipment order was ever signed. I hope as I briefly tell about how we got here some of those principles will aid you in assisting the public safety community to achieve this sometimes-illusive goal of being able to communicate with each other.

How Did We Get Here?

We identified a "Common Problem" which brought the stakeholders together. This was done without concern as to whether there would be a final product. It simply brought the potential users of a combined network together to get the issue on the table. A convener of stature brought us together—in this case it was our Governor.

A committed leader was appointed to broker the effort and focus on keeping the effort together. All meetings were held with openness, transparency and with voluntary participation. The effort utilized committed decision makers who came to the table to make commitments.

There was a set of clearly defined purposes and goals, a predicable management and maintenance process. A formal charter was developed: it outlined governance, outcomes, funding and levels of participation. Legislation was passed to memorialize and charter the effort for long-term results.

We recognized that this is not a problem with a one-time fix. It will require nurturing and management, because the problem is here to stay and will be come a part of a long-term organizational management process requiring ongoing resources.

After all these issues, directions and organizational efforts—then we talked about the money, and possible funding mechanisms.

So what does all this have to do with the Homeland Security Sub-Committee on Emergency Preparedness, Science and Technology?

Let me share with you the following:

It has been said that: "During times of emergency, people expect government at all levels to provide the appropriate response to mitigate disaster, save lives, provide support, help the needy and care for the injured. The major tool in providing that response is a communications system with reliable and dependable capabilities and capacity". There is simply no room for error. The communications system must rise to the occasion at a moments notice—and be prepared to sustain the highest degree of operability for whatever the duration of the situation will be—whether it is a multi-car freeway accident or a sustained attack on our country. It will then go back to supporting day-to-day traffic loading until the next emergency.

The citizens we serve expect in today's world of miraculous technology that this is what will take place. Sadly, in many instances it may not. While some areas of the county have progressed, many are still searching for answers.

Why is that so?

The public safety market is a limited demand market with a focused product line. The equipment is costly to procure, install, maintain and upgrade. Typical public safety systems have to last a minimum of 10 years with many working well into thirty years. This makes it so difficult to overcome the technology curve. The system must be installed in protected hardened environments with redundant connections. It must be prepared to operate in the highest of demand. Because of its limited market presence, the cost of the individual units and the infrastructure is very high.

A public safety system falls behind the "other needs of government". Roads, social services, police cars, fire equipment, staffing and training all take precedence over the expensive proposition of funding a public safety radio system. Many times when funding is set aside it comes from limited resources or one-time allotments. There never seems to be sustainable sources to keep the effort fully funded, progressing to a solution and fully maintained.

There is a high degree of resistance from public safety agencies supported by age-old political barriers that create roadblocks in motivating agencies to work together and share a system and the associated costs. Cities, counties, states, and yes, federal agencies in some instances cannot find the common ground on which to chart the course and build a common communications infrastructure to support them all, giving the autonomy they need and the interoperability they desire, when it is needed. There is also reluctance between fire departments, police departments, and EMS providers to share resources and communications systems, because of the presumed loss of control.

In multi-agency endeavors there is a reluctance of one governmental agency to spend its tax dollars supporting a system located across multiple jurisdictions because their agency should not have to pay to support services in another city or county. We have run into this problem with our own system when justifying expansion into areas to support state users.

Bringing agencies together requires a unique "governance" structure for operation, implementation and maintenance of the communications system. Many governmental agencies cannot or will not participate in these unique organizations.

So what can this Committee do to assist public safety to achieve this interoperable goal? Take a leadership role and support the SAFECOM program. This program is the DHS effort to promote interoperability. They cannot do it without proper staff, funding and a direction and mission.

With appropriate resources, SAFECOM can and should staff up with state and local experienced personnel who have the background in communications to assist in the process. SAFECOM needs to be able to provide the resources to take the interoperability message nation wide. It should be able to host instructional seminars focused at state, local and federal partnerships to develop a dialogue among users and future partners. These forums will allow for the exchange of ideas and instructions to regions beginning interoperability projects. SAFECOM should develop resource tools for use by agencies such as case studies, how to guides, success stories available to those starting the interoperability process.

The federal government should also tie future federal funding to performance measures. Give priority attention to multi-agency, multi-discipline projects with long-term goals and reasonable chances to succeed with long-term results. Have the grant requests reviewed by peer groups who are familiar with successful projects before awards are made.

The government should reward innovative projects and highlight them at association events (APCO, IACP, IAFC), sending the message that funding is tied to cooperative efforts. Future investments of federal dollars must equal measurable results. Any grants must have a definable purpose and expected outcomes.

Congress should establish long term sustainable funding to support the public safety effort. This problem will not go away in a few years. It is a long-term commitment that will take continued to sustain and support.

Congress should also push, sustain and provide funding to motivate the standards efforts. The quicker manufacturers have a set of standards to build systems to, the quicker we have a larger selection of user devices (handheld and mobiles), and component infrastructure pieces the more effective and interoperable public safety systems.

I am quite sure these are points you have already listened to. However in actuality, they are the keys to success. While they are an important part of the process, this problem will not go away with more frequencies and more money. What is required is true leadership, vision, and bringing together of all the players and resources to make better operability and interoperability possible.

Thank you. I will gladly take any questions you might have.

Mr. REICHERT. Thank you, Mr. Proctor.

I have a few questions. There will be a vote that will be called, I am told, in the next 15 or so minutes, and we may have to recess for a brief amount of time to allow everyone to ask questions.

Mr. Proctor, you summed it all up pretty well. Support SAFECOM, performance measures, innovative projects need to be identified, regional projects and partnerships need to be identified, long-term funding and support, and motivate people who are meeting all those standards and requirements that you laid out.

One of the things that we are doing in this subcommittee is that we are going to have all of the testimony evaluated. We started back before Christmas looking at operability first. I think the chief mentioned operable, we must be operable first. We are taking a look at every statement, every answer that is given to this committee, and we are going to draft legislation that addresses the issues that you just talked about, all four of the witnesses.

But I want to follow up just a little bit further and maybe get some specific answers from anyone who chooses to answer the first question. Do you believe that the Department of Homeland Security sufficiently supports SAFECOM and the Office of Interoperability and Compatibility, honestly? Anyone?

Mr. PROCTOR. I personally believe the SAFECOM project needs more support. I think they are severely understaffed, I think they have good ideas, great direction, and many of the things we did before SAFECOM was even invented are the things SAFECOM is now using now and trying to promote. I think it is key that that message be taken around the country in regional seminars, in big cities so that people can come together, begin talking, learning, establishing priorities, working together. Those relationship that Charles talked about are critical in developing interoperability communications. Technology is easy; it is the relationships that are difficult to form.

Mr. REICHERT. Right.

Chief?

Chief WERNER. I guess to add to that, if you look at the monumental task that has been laid out to accomplish and the expectations that are there, I would argue, if you evaluate the desire that you hope to accomplish and you evaluate the resources that are in place, that might answer the question that you are looking to have answered.

Mr. REICHERT. We do know that there are authorized 16—in the Office of Interoperability, 16 FTEs, and they now have 4 working in that office.

Anyone else want to answer the question about SAFECOM and interoperability?

Mr. DRAKE. Mr. Chairman, members, thank you. The application would be the same as it would be on a local basis with the funding for this effort. You need to prioritize. I think my colleagues have made the case today for you to promote interoperability and operability. And I am the newest member of the SAFECOM Committee, but it did not take me long to realize that the committee is understaffed, the effort, while well-intended, will not wash out in local government and will not wash out back in your districts and mine and back in my city.

Talk is cheap, and if this is not funded, the collective effort is not given, the next disaster will come and everybody will be throwing up their hands and pointing, and you control the ability here to not have that happen. So I would suggest further funding.

Mr. REICHERT. In your dealings with the federal government and helping you build your system from the ground up, is there any one federal official that in your view is accountable for interoperability? Yes or no?

Mr. Proctor?

Mr. PROCTOR. In our process prior to the Olympics, we worked with six or seven different agencies for assistance besides the 120 agencies we have at home. So it is a multi set of tasks.

Mr. REICHERT. So the answer would be, no, I am taking it, from the panel. If there is not, should there be?

Chief WERNER. Well, to answer your question, no, I do not think so. And because, as you mentioned, if you take a look at how many agencies are involved in the interoperability at the federal level, I am not really sure there is an assignment that is specifically given and authorized to take that accountability. Should there be? Certainly.

Mr. REICHERT. Anyone else? No?

Do you believe the federal government's efforts are well coordinated as they worked with you? Anyone on the panel?

Mr. MENCHINI. Commissioner Menchini here. We really have been appreciative of SAFECOM's efforts, especially in the area of data communications, to publish statements of requirements that begin to provide much needed leadership to be able to get common infrastructure in place.

And we have made our feelings on this known, that we really believe that each area needs to be very carefully considered in terms of its particular requirements for operability and for interoperability. And there is not one particular approach that really can be applicable across the nation.

Mr. REICHERT. Right.

Mr. MENCHINI. In fact, it really has to be a grassroots type of an effort with, and being driven, as I have heard here at the table, by the requirements of the first responders based on their operational needs, based on the particular threats that they have to deal with, and interoperability and operable systems need to be built from the ground up. So whatever happens at a national level and the need for strategy is clear, but it does need to be based on a variety of different types of models. Again, large cities, I think, very much are different types of environments for radio communications as well as for first responders operations.

Mr. REICHERT. I would agree with that.

The Chair recognizes Ms. Harman.

Ms. HARMAN. Thank you all for your testimony. It is very interesting, and it is clear to me that you are all enormously qualified in your own rights, but the stories you have told us show that local and state agencies are ahead of the federal government on this issue. And I worry about that.

I was thinking about the four S's here: Strategy, spectrum, standards and sustained support. It seems to me that might cover some of the gaps in the federal response.

I just want to ask you a couple things, just as the chairman did, and ask any of you to answer.

The first is big state, little state, big city, little city, sure, there are differences. I come from a big city, and New York City would certainly qualify as that. Maybe some of the Portland cities would be considered smaller, maybe, but their west coast cities; therefore, they are very important.

But, seriously, should we have different approaches or is it rather that each approach needs to be considered as part of this national strategy? For example, should we have a catastrophic attack that perhaps is avian flu—let's pick something horrible—that would hit all of us, maybe one region at a time, but that region would have big places and little places.

When we think about strategy, shouldn't we include both small and big in the strategy?

Chief WERNER. I think that the approach to evaluating the situation can be very similar, and I think that you can also identify outcomes that you hope to achieve as being very similar. I think the method or the medium to which that gets you there can be very uniquely different based on geographic region. So I think if you take a methodology and use it to help evaluate and give you a vision, that can be standardized and institutionalized. But, as my colleague here from New York has mentioned, there are some very unique things that have to be addressed in each locality.

Mr. DRAKE. Congresswoman, I think a basic framework is essential because whether the flu hits my city, Beaverton is 83,500, or Portland, which is about 525,000, we will share the same problem, and my children will react the same way to the flu as someone in Portland will.

We need the flexibility to be able to respond individually, and the National League would always argue that, "Give us a basic framework, give us general guidelines, but let us implement it that works best for each one of us."

As a past president of the League of Oregon Cities, I represented cities from—actually have 241 cities in Oregon, 2 were ghost towns with no population, but the smallest actual city had 25. And between 25 and 525,000, there are a lot of cities that ranged in size, but when we would approach the legislature we would ask for a general framework but always allowed to implement it on a local basis.

Ms. HARMAN. Thank you.

Mr. MENCHINI. I would have to—I am sorry.

Ms. HARMAN. Go ahead.

Mr. MENCHINI. I would have to agree, and I think it is really a matter of local-based solutions based on local needs but a common set of requirements and a common set of expectations.

Ms. HARMAN. Thank you.

My second question is about spectrum. I would like to thank all your organizations for supporting the HERO Act. The League has done this, the international fire and police organizations have done it, I think the National Governors Association has done it. The problem is, Congress has not done it. And we will be turning over analog spectrum, as some of you mentioned, in 2009. That is 3 years from now.

My question to you is, in those 3 years, tell me about the challenges you are going to face. Some of you have described this, why spectrum matters, but for those who have not, here is an additional opportunity to rail against Congress' inaction here about the problems you are going to have for 3 years without common, dedicated emergency spectrum.

Mr. MENCHINI. I can answer. In regard to New York City, we are faced with a challenge of addressing our broadband data requirements without the benefit of the 700 megahertz spectrum. So we are now building out—the first pilot areas are going up as we speak, building out a citywide broadband wireless network. We have had to do that with spectrum that we were actually leasing from the archdiocese of New York to be able to get the type of spectrum that we need to be able to support public safety data requirements. So the 700 megahertz spectrum cannot come soon enough.

I think there needs to be a constant eye on the evolving needs of public safety and a look out even beyond the 2009 timeframe and the availability of a 700 megahertz spectrum to keep the availability of spectrum in line with the needs of public safety responders.

Ms. HARMAN. Any other responses? My time is expired, but I know the chairman will let you answer.

Mr. PROCTOR. I would just like to echo what my colleague has said from New York City. We, too, are building out a 700 megahertz data system. We are using the state licensed 700 megahertz spectrum and appreciate it so greatly because there was no other place to go. And we look forward in completing our plan and being able to use the balance of that spectrum very soon to enhance our system operations.

Ms. HARMAN. Anyone else?

Mr. DRAKE. Yes, Congresswoman. We are all, at least I am the only elected, I believe, at this table, and you are all elected. We represent real people and real constituents, and there is no excuse for politic or anything else when it comes to public safety. We have within our power and authority, you certainly have within yours, to implement this sooner. The National League would always encourage you to deal with this sooner than later.

Mr. REICHERT. Thank you.

Ms. Lowey?

Mrs. LOWEY. Thank you, Mr. Chairman.

I want to thank all of you for your testimony, and I want to especially thank the chairman and the ranking member for their bipartisanship.

And you should know, if you have not appeared before our committee before, many of us have been talking about interoperability for a very long time. We have introduced legislation, we have tried to move the Department of Homeland Security, and yet with 180,000, I believe, people at the Department of Homeland Security, whether it is four or five, I am not sure who has been hired or fired today, we still do not feel that there is a serious commitment. And I do appreciate the chairman having this hearing.

Following up on the questions before, one of the questions I have had following up with Katrina is that a backup communications system really is essential and could be invaluable. I think it is safe to assume that in a catastrophic incident there could be serious damage to communications infrastructure. And a backup system might enable lines of communication to remain open, even if the major network is inoperable.

Perhaps I would begin with our commissioner in New York City and then you could all respond. I wonder if any of the areas you represent have a sufficient backup system. Do you have a backup system? Are there any promising technologies that should be examined by this committee or are being examined to see if a backup system is feasible and can be effective? I would be most appreciative, beginning with the commissioner.

Mr. MENCHINI. Well, I think the events last year in the Gulf area are really telling. In fact, in New York City, we had a different type of a problem 2 years ago when we had a blackout that also created a very similar situation where we lost power citywide in some areas for over 22 hours. That put strain on telecommunications infrastructure, on telco infrastructure, on cellular infrastructure, on public safety radio infrastructure. It is probably very similar. I mean, it is a shorter period of time, but it is similar, in effect, to what we saw in the Gulf area.

So the ability for us to implement at an infrastructure level very robust, very survivable and redundant radio infrastructure to be able to survive power outages caused by blackouts or caused by natural events like hurricanes is a critical area that requires a lot more investment and the applicability of known methods.

You just need to be able to have, in addition to a battery backup, the ability to be able to roll generators up, if need be, or have a much extended battery life for your different components that are out there acting as receivers and transmitters, for example, in a radio infrastructure environment.

So we have seen something like that in New York City. We have taken steps to be able to do what we can to be able to reinforce the infrastructure. But I think there is still a lot more that needs to be done, and if we have learned anything as a result of the events in the Gulf area, having radio infrastructure that can survive those types of events and give us operability first and then interoperability is critical.

Mrs. LOWEY. Anybody else care to comment?

Yes, sir.

Mr. PROCTOR. We have done many things as we have developed our system. For instance, we put two paths of control communications in every site so that if one fails, we have a redundant link going in. We house fuel and generators at the site that will allow

them to operate for 7 days without having to be visited. We put redundant transmitter facilities on different mountaintops . I do not know how familiar you are with the geography of Utah, but most of our facilities are built on mountaintops rather than on the tops of buildings. We have different mountaintops built into the network, so that if one fails, we immediately route to another one.

And all those battery backups, uninterruptible power supplies are critical. Good grounding, we take a lot of lightening on tops of mountains. We have good grounding systems to ensure that the equipment is properly grounded. And good installation procedures to make sure it is installed properly.

It has never failed to amaze me how many agencies will install $1 million worth of equipment in an old shanty on top of a mountain and expect it to function properly over a 20-year lifespan. We have tried to avoid that.

Mrs. LOWEY. Thank you.

Chief WERNER. I guess I would like to add that in the catastrophic situation that occurred in Katrina, which was really unusual as far as the amount of infrastructure that was affected, one thing that might also be considered because a total redundant system is going to become very expensive, and when we are trying to get operable and interoperable systems to begin with and thinking about getting backup systems to go in place, there is just not going to be enough money to do that.

One of the things that we might want to think about is to have some type of tactical equipment being set up quickly, infrastructure, in areas that we know are prone to major disasters. For example, have something—I know Florida has some things where they drop pods right in place, get the transmitters in place and allow people to begin communicating when everything is gone. And I think that is one of the new things that we have not really planned for.

If we had some of these things strategically placed that could be pulled in in a certain amount of time that we define as acceptable, that might be an alternative solution.

Mrs. LOWEY. Thank you. My time is up.

Thank you, Mr. Chairman.

Mr. ETHERIDGE. Mr. Chairman, thank you, and let me associate myself with Ms. Lowey's comments as it relates to thanking the chairman for calling this hearing, because I think all of us see this as a critical weakness in our emergency response systems.

Since the terrorist attack of 9/11, it really exposed a very serious problem, and Katrina laid it bare once again, the lack of a backup.

The federal government promised to devote more resources to solve the critical problem, and while some of the funding has increased, recent DHS budgets have focused on border security and other issues that were out there that tend to get more attention.

In fact, the Republican chairman of the Senate Budget Committee is quoted in the morning Congressional Daily as saying, "The Bush administration has paid scant attention to homeland security."

So I am pleased, Mr. Chairman, that on a bipartisan basis we are going to address this and hopefully apply the lessons we

learned on 9/11 as it relates to operability and interoperability, finally.

In previous hearings on interoperability, many of the witnesses contended that there is a lack of leadership on the federal and state levels on this issue. However, it appears that in some areas of the country local first responders groups do not always appreciate bias and direction from officials at a higher level, whether that be state or otherwise. We are trying to develop a statewide system or a regional system.

Would you share with us your views on this issue and how you think communications and cooperation between state and localities can be improved, which I think is critical if we are going to make it work.

Chief WERNER. I agree. I think it goes back again to this methodology of developing the relationships first and creating a partnership. And one thing I would urge that we have learned in Virginia is that it is important that you have practitioners involved in what those solutions are and that you listen to them and help develop whatever it is that you are going to put in place and not come across as a dictator of how it is going to be and you are going to accept this solution or here it is, take it or leave it.

Mr. PROCTOR. Prior to establishing our agency and constructing our network, we literally took a road show around the state and talked to every city and county, sheriffs and police chiefs at conventions and asked them what they needed to see. How do we do this? What can we do to best serve your needs?

And as we went through that process, there were a lot of them who pushed back and did not want to be part of it, and there were some who came, immediately stepped forward and wanted to be a leadership person in it. And we capitalized on those, we moved forward with those who would be a part of it, and it was interesting to see that the rest after the system came full circle they came back around and wanted to join up.

Mr. ETHERIDGE. Anybody else want to comment?

Mr. DRAKE. Yes, Congressman. Some states are certainly ahead of others in terms of the cooperative effort. Oregon's SIEC is bottom-up and top-down and is well integrated. I think more and more of the states are beginning to do this. And, again, I think we are all learning from our experiences. We would welcome the leadership on a local level without being given a straight jacket.

And I guess I would offer that those who are moving in the right direction be awarded an rewarded for their effort, and those that are not, one way or another, by the positive-negative incentives, they would eventually come to the table.

Mr. ETHERIDGE. Do you agree?

Let me ask one final question, because I know we are running out of time. Secretary Chertoff said earlier—and I know some of you wanted to comment on this—said the states were getting funds now about additional funding. Would you care to comment on that?

I raised the issue with him that there a lot of those funds in the pipeline and they have pretty stringent requirements. Any of you want to comment on that?

Mr. MENCHINI. I think it is also important to note what type of financial challenges localities and states are facing in regard to their radio requirements.

Mr. ETHERIDGE. Right.

Mr. MENCHINI. One thing many of us have, aging radio infrastructure that we are already dealing with that need to be replaced. But the requirements of interoperability are bringing more and more public safety and first responder users onto our radio infrastructure is stressing those networks. The need for us to make them more survivable and the need for us to meet FCC requirements for narrow banding as well as to be able to implement 700 megahertz radio frequencies and to begin to move broadband data capabilities to our first responders is a tremendous set of undertakings that will have huge cost implications for localities.

The needs, I think, are really snowballing, and I do not think any area is able to keep up without tremendous expenditures that will have to come from other areas of government.

Chief WERNER. If I may add something really quick, what I see is if we are looking at the state grants, I do not think any of us at this point know what our state grants will be now since the federal grant process has changed. With the vulnerability and risk, a device has now been put in place. The numbers are going to change, and if you think that the money that is being given now to states is going to be enough to achieve interoperability it is not.

Mr. ETHERIDGE. Thank you, Mr. Chairman. I yield back.

Thank you.

Mr. REICHERT. Well, it is just you and me.

[Laughter.]

I am going to make this public announcement. I am going to miss this vote. We are going to wait for Mr. Dicks to come back. I think he had a couple of questions. I have a couple more questions. The votes was a vote honoring the service of Justice Sandra Day O'Connor. Of course, my vote certainly would have been a yes vote in honoring her service to this nation. We will make a public record when we go back to the floor of House later.

I wanted to follow up on a couple of things. You talked a lot about—I think it was last week I was in Portland and we chaired a subcommittee hearing on health IT. And one of the witnesses there testified that there were nearly 800 vendors of different technologies that touched on just about every problem that you could think of that may be associated with just the health IT interoperable discussion.

I imagine there are at least 800 or more vendors out there with different technologies. In your four jurisdictions how did you deal with the different myriad of options and choices when it comes to the technology decisions that you made?

Mr. DRAKE. Mr. Chairman, there partly lies the whole crux of the issue that for many systems, both for us in the Portland area and I know speaking on behalf of many jurisdictions in the state, you are not looking to new technologies and new systems. You are looking for ways to bridge the gap.

The real difficulty, I think, for us on a local basis is either the ability to find a patch to get us there or finding the barebones system. And you do not have the luxury, I do not care what the issue

is, it could be interoperability, it could be anything, you ca not just start musing and think, "What is it I would like to get," and start exploring. Part of it is this is America, so the vendors come to you, but it also is just the fact that—

Mr. REICHERT. Sorry.

Mr. DRAKE. That is okay.

Thank you, Mr. Chairman. The fact is, is that there is going to be a basic technology you are working with, and I think Mr. Menchini touched on it, that there is difficulty in many cities, many areas just to afford the basics. And whether you are just trying to get to the next technology, in many cases you ca not afford to buy that next system; you look for the patch.

So my comment would be that there are plenty of places you can go in terms of expertise to find out what the right system is, but the real issue initially is, can you afford to even do that patch? And looking ahead to the next technology, in many cases, is very difficult.

Mr. REICHERT. I was just consulting there briefly. There are 38 police departments within the King County, the county where I was sheriff in Seattle, and there were a couple of smaller police departments that purchased a system, more of an information communications system, I suppose, and it failed. So they spent $1 million or $2 million in these small cities and it crumbled on them.

So I guess there is this fear, I think, that at least in some areas where there is technology out there and there is a sales job and it looks good, they pay for it, and it blows up in their face. And that is, kind of, you know, how do you weed that sort of—

Mr. DRAKE. Mr. Chairman, I would defer after a quick comment to my colleagues who have the technical expertise. But therein lies some of our request in that we get some basic framework in terms of general guidelines, and I think that would take care of some of that concern that you would have.

Mr. REICHERT. Thank you.

Chief WERNER. What I think is a part of the question you are asking is defining what it is that you want the system to do and then trying to encourage as many people to be a part of that system. And, fortunately—or unfortunately, or however it may be perceived—the cost of radio systems, as we know them today, to meet the requirements that we are hoping to achieve, are very expensive.

What we did in our locality in the regional perspective is that all the agencies in the three jurisdictions came together to do one radio system, which helped to share the cost between the three. How do you get there? It is defining the specifications as specifically as you can and making sure that you have as best an iron clad contract that you can when you negotiate it. And even then you are not guaranteed that the system that you get will be what you thought it was going to be.

Mr. REICHERT. In your opinion, should the National Telecom Communications and Information Administration have responsibility for administering a $1 billion grant program for interoperability?

Chief WERNER. I guess I will address this first. I guess I would question why we bring in another agency on top of the myriad of

other agencies that have been involved with interoperability? Why are we adding one more layer of someone who has not been involved in this particular discussion?

Mr. REICHERT. Yes. I hope you notice that some of the question I am asking I know the answers to already. I do not want you to get the idea—Mr. Dicks arrived just in time.

Mr. Dicks?

Mr. DICKS. Thank you, Mr. Chairman. And I want to compliment you for holding this hearing. I think this is very important, and I appreciate the excellent testimony we have had here today.

What happens, Chief, in a situation where you do not have any cells, where you are in an area where it is blank and you need to be able to communicate? The reason I raise this, there is a company, I think, in your district in Kirkland that has come up with a way of using wireless and then in a dead zone they connect up to the iridium satellite.

Now, would that work? I mean, does that sound plausible to you?

Chief WERNER. Well, it depends on the level of communications that you are talking about. Typically, when you are talking about satellite communications, it is not a good tactical solution because of delays, latency of transmissions, the amount of capacity that can be in place. As far as some singular command issues and communications between them, it probably is a good alternative.

Moreover, I would think that if you have areas that do not have coverage, an alternative would be some type of transportable tower site that can give you communications within a region to a cache of radios that allows multiple agencies to work. I think this is probably similar to what Forestry has done on many occasions.

I think that we have seen that Forestry has been one of those areas that has to deal with the very unique logistics of being in the middle of nowhere and having to communicate and deal with some very large incidents.

Mr. DICKS. And how do they do that again?

Chief WERNER. Well, in some cases, they will bring their own portable towers that are radio—

Mr. DICKS. Oh, that is right. That is right.

Mr. MENCHINI. Actually, in New York City, we have an erectable system, tractor trailer-based that can be rolled to a hilltop in Central Park, wherever we need to be able to provide additional coverage and a cache of 500 radios that can be supported by that system. We keep that on standby, and even though our infrastructure can support communications, in the event that we need to have that type of portable capability, we can roll that in and deploy that very rapidly.

Mr. DICKS. But not everybody has that, right?

Mr. MENCHINI. No. We acquired after September 11.

Mr. DICKS. Tell me about SAFECOM. I mean, I get the impression that they are trying to help you, but they are not adequately staffed, they are not adequately funded, and, therefore, they are not able to help all the communities that need to be helped.

Yes. Mr. Proctor?

Mr. PROCTOR. I believe that to be the case. I believe the SAFECOM Program is a good effort. I believe they are focused on some of the things we need to get done. I think they desperately

to hire staff up, hopefully getting some support from state and local communities, as people change jobs and change careers, that will give them some direction from the ground up level to help them focus more on the interoperability issues.

The Executive Committee, which I am a part of and Charles has been a part of and the mayor is a part of, has worked wonders so far in getting this thing off the ground. But they just physically do not have the people to march through the bureaucracy of government to get the message down to the lowest level, which are the states, cities and counties.

And one of the programs previous to the SAFECOM Program was called the FSWIN Program, and it took the message out to the cities and counties. They held regional meetings and that was so critical because it brought people together. It started the conversation, it started the interaction, one with another, and it started—

Mr. DICKS. So that is not happening now?

Mr. PROCTOR. No, it is not.

Mr. DICKS. Unless the region does it itself.

Mr. PROCTOR. That is correct.

Mr. DICKS. Mayor Drake, isn't that basically what you have tried to do down in the Portland area?

Mr. DRAKE. Yes, Congressman, and, again, being the newest member of SAFECOM, I did all the brushing up I could do prior to joining the committee, and I was flabbergasted. I like lean and that is how I operate my city, but it was skeletal. And I think the chairman correctly stated that it is permitted to be staffed at a much higher level.

Mr. DICKS. Well, and the point is, why isn't it staffed then? I mean, do you have any idea why they have not gotten more people on board? Is it a lack of will or commitment or it just takes time? When was SAFECOM stood up? When did they start this operation?

Mr. DRAKE. I believe it is about 3 years old, 3.5 years old.

Mr. DICKS. And not to be partisan, and I am probably one of the least partisan people you will meet, but this is Congress. This is not the only area in the Department of Homeland Security that has gotten off to a very slow start. So one has to wonder whether there is just not the effort being placed or the commitment of resources or the willingness to go out and get these things up and running. That takes leadership, as you all four represent leaders who have done it in your area. It takes some commitment from either the White House or Mr. Chertoff's position or whoever's in charge. Dr. David Boyd, is he the person?

I mean, it takes somebody that says, "We have got to get this done." And that is what worries me is that this thing has dragged on and we are not getting the resources out to the local communities, and it is not happening.

Now, who is supposed to evaluate all this technology? I mean, everybody's out there working on coming up with solutions. We have got several companies in our own state of Washington that are coming out, one with a software solution and others with wireless, using satellites. I mean, who evaluates this? Is Homeland Security in a position, the science aspects of Homeland Security to do this or does it happen at the local level? Is it just, kind of, every-

body goes out and presents their technology and it is utilized in some places? How is that working?

Mr. MENCHINI. I think it is essential for that to occur at a local level. And, again, I think first responders, public safety officials in a local area are the only ones that really know what their needs are and really would only be able to determine whether or not a particular technology—and as you have mentioned, there are so many different technologies and more arriving every day. How that fits into the needs of a locality can only be determined by the locality itself.

Mr. DICKS. So you think that is the best way to do it. They should evaluate, they should—

Mr. MENCHINI. Well, let me qualify that.

Mr. DICKS. Because you have got each situation is different. Maybe some things will work in one situation when they might not work at another place.

Mr. MENCHINI. I mean, I think it depends on the locality as well. There are some localities, and you mentioned before, the chairman, what happens when monies are invented and a particular solution is not successful. A lot of it has to do with the fact that in addition to the monies that are needed to acquire these systems, there needs to be technical staff and people in that locality that understand these technologies—and, again, they are changing very rapidly—and understand how to implement them.

So there is a need for local knowledge, and where that local knowledge does not exist, I think there might be some other solutions that need to be considered. But it is not a one-solution-fits-all.

Mr. DICKS. How many staff people do you all have in your office working on these issues? You are the staff, right?

Mr. PROCTOR. We run a system that has over 500 repeaters located on mountaintops, over the half state of Utah. We have one director, four technicians and one operations manager, a secretary and an administrative assistant.

Mr. DICKS. So seven or eight people you are talking about.

Mr. PROCTOR. That is right. If there are issues with system problems or things that come up that we ca not handle, we hire it on a contractual level.

One other thing I wanted to say in defense of Dr. Boyd and the SAFECOM Program, I think part of the issue why this has not organized and boiled up to the top is simply all of the changes that are taking place in the Department of Homeland Security and all that consolidation and effort that has gone on, I mean, these folks have had to take this program forward as fast as they can and get something out on the street. And they have been successful in doing that, using resources like the EC and the contractors they have to help.

It takes time, it takes a lot of time to go through a hiring process to get qualified people to be a part of your staff. Coming from a state government level, I understand that. It takes about 2 to 3 months to hire somebody. And I just think they need to get with it and get moving forward to take care of that. And part of the issue is, is they have got so many things on their plate now—

Mr. DICKS. And they have got to find good people too. You have got to have people who have some background.

Mr. PROCTOR. That is exactly right. And having just recently gone through a hiring process for some technical staff, that pool of technically oriented public safety personnel is willowing drastically. It is drying up quickly as people retire. People like me who grew up in the systems go on to other things and retire.

Mr. DICKS. I would assume the contractors are hiring up some of these people—

Mr. PROCTOR. That is correct.

Mr. DICKS. —the people that are trying to market this equipment.

Mr. PROCTOR. That is correct. They will go to places where they make more money. A cell company will pay a radio technician a lot more than a government agency will and give him all the overtime that he can use.

Mr. DICKS. Chief, how many people do you have working on this?

Chief WERNER. Well, if you look at the state efforts, there are two people, and if you look at our local efforts, we are talking about three people. And I guess if you take that in perspective and say if the state of Virginia is doing their effort of guidance with two people and we are doing our coordination with three people and Steve is using seven or eight people and you reflect that on the national level, would that give you some perspective of how short we are at the national level with staffing?

Mr. DICKS. It certainly would.

Mr. Menchini?

Mr. MENCHINI. Well, when you say, "people dedicated to this," do you mean to interoperability?

Mr. DICKS. Yes.

Mr. MENCHINI. Or to radio infrastructure as a whole?

Mr. DICKS. Well, you know, the whole picture.

Mr. MENCHINI. The whole picture is one—I mean, we worked very—

Mr. DICKS. New York's got a lot of people.

Mr. MENCHINI. We are large.

Mr. DICKS. Yes.

Mr. MENCHINI. We are going to be very different, I think, than some of the other people here at this table. Again, we have 40,000 police officers alone that are protecting New York City. And we have approached this, I mean, first of all, with—and I have the benefit of Mayor Michael R. Bloomberg who gets technology and understands the role that it can play in supporting not only public safety but regular government operations.

Commissioner Raymond Kelly from the police department, Commissioner Nick Scoppetta from the fire department, and Joe Bruno from the Office of Emergency Management. It is very much a team and collaborative effort.

So I think we had direction from the top to be able to address our interoperable radio requirements and to work as a team. And as a result, the entire radio group, each of those departments. Have been dedicated towards the planning and implementation process, which has resulted in a lot of achievements.

So it is not just a matter of a group dedicated to interoperability, but it is really incorporating the need for interoperability into the overall radio infrastructure development and rollout. We are about to implement—in fact, one of our next pieces in getting to where we want to be to support interoperability is to move our fire trucks themselves onto the same UHF infrastructure that our walkie-talkies are now on. So that I can turn from a fire truck, turn a channel and be on the same channel as the fire fighters going into a fire. That project is—actually, a contract was just awarded to Motorola for $75 million to build that infrastructure throughout New York City. We have a mob of people walking to be able to implement that.

But, again, a strategy that once implemented made every action of our various radio people moving down a path toward accomplishing interoperability.

So, again, I am a different situation, but I think it is key to have a vision, have the leadership and support from leadership and to be able to make every step and every investment that you make in line with where you want to be. I do not know if that answered your question, but—

Mr. DICKS. Yes. That was good.

Mr. MENCHINI. Okay.

Mr. DICKS. Mayor?

Mr. DRAKE. Congressman, thank you. The first request from the National League of Cities is to elevate SAFECOM, and I would guess being the newbie coming in but understanding politics, if you are not funding something to the level it should be and more so giving it the recognition it needs, there may be difficulty in getting people to complete the task that SAFECOM is supposed to complete.

Mr. DICKS. They do not think that there is a real dedication.

Mr. DRAKE. Well, that would be, I think, NLC's guess that it is not getting the visibility and recognition it deserves, and there are so many cities across the country that do not have the expertise. We do things in a collective way, not only in my county, I chair our county's 911 Board and in the region we collectively talk about the technology. But SAFECOM is there to give some national guidelines, but if it is not elevated to the level it should be, I think Dr. Boyd's hands are tied then.

Mr. DICKS. So you are not getting guidelines? You are not getting a lot of input from the national level?

Mr. DRAKE. Congressman, I do not think we are getting what we need from SAFECOM, and the NLC is asking that SAFECOM be given the recognition and the support that it needs to do just what you are asking.

Mr. DICKS. Thank you, Mr. Chairman.

Mr. REICHERT. Well, Mr. Dicks and I are from the same state, the state of Washington, and this is my first term in Congress. We are in the United States Congress, and now that we are here together, we are going to get some things done, right?

Mr. DICKS. That is right. And I have been here 15 terms and I have never been chairman, so you started off on the right team.

[Laughter.]

Mr. REICHERT. Well, you can always become an R, I guess.

[Laughter.]

Mr. DICKS. I do not think this is the right time for that.

[Laughter.]

Mr. REICHERT. So you can see we can have some fun even.

We are really serious, though, about this interoperability effort. This is a committee, and as I think you saw from previous questions and the previous members' questions, that there is a real, real deep interest here to make things happen for our first responders across this country. And it is not just about interoperability. It is about operability first. It is about interoperability, not just with our fire departments, EMS, emergency managers and police departments, but it is also coordinating the ability to communicate with businesses and to others now that we recognize Department of Defense, et cetera.

So all of those things are now a part of our discussion around interoperability. But we have got to start somewhere. And some of the things that you have mentioned, I mean, it all starts with leadership. So we recognize that leadership is the first thing, and Mr. Dicks spoke about leadership in the Department of Homeland Security. We recognize there is a weakness there.

We recognize that there are some good things that SAFECOM has done and at the Office of Interoperability has done and will continue to do, but we need to be there to help them push this forward.

And what I also hear loud and clear—and there were a list of things that I listed off earlier that Mr. Proctor touched on, I will not go through those again—but loud and clear, each system has to fit the community and the needs of the community. I know that, you know that, we all recognize that fact. I see it very much like the community-oriented policing programs that were started back years ago. Of course, most cops were a little bit nervous about community-oriented policing. As one of those people back them, I was too.

But it is the way that that system was set up in a way to across the nation set a standard and have performance measures and have grants attached with the performance that police agencies across the nation were required to meet that were molded to the specific communities. And that is the key with interoperability.

I want to let you know that your testimony, although now this room is rather bare of members of Congress, is very important and very key. Your presence here today is going to get the ball rolling. As with the other witnesses who have appeared before, will move this issue forward. Your role today will be an integral part of making interoperability a reality in this nation.

So both of us who are still here would like to thank you so much for your testimony and taking time out of your busy schedule to be here.

Chief, you have the last word.

Chief WERNER. I just would like to say thank you all for letting us come and speak. And one thing I would like to reinforce is that the one thing that has really been a good thing that SAFECOM has done that must be noted is the continuity of grant guidance when it comes to interoperable communications equipment. There needs to be one force that decides those guidance standards that

go across every agency that has that money, so that we do not have fragmented and different understandings of how that money should be spent.

Mr. REICHERT. Okay.

Yes, sir.

Mr. MENCHINI. I would have one message that I would like to leave. One of the real challenges for us has been that we have had to react to the grants that are available rather than there being a dialogue with us as to where our needs are. It is not my needs, I am in a support role, but where the needs of first responders are and to have the grants designed to be able to meet those needs and to have, I think, if SAFECOM can play this role, that would be terrific, but to have more of a voice in where grants are available so that when monies do become available through a grant process, it is more targeted towards where the actual needs are.

Mr. REICHERT. But you do not want them to tell you what you have to buy, do you?

Mr. MENCHINI. No.

Mr. REICHERT. Wouldn't you like to have some flexibility to decide what it is that you are going to—

Mr. MENCHINI. Again, what I think we need to do is to hear from first responders as to what the problem is that we are trying to address before we get down to a particular solution. And then we can talk about having standards, which, again, is a double-edged sword by getting to a point where the solutions can be available from the marketplace and can address a need. But it should really be driven from the need, as articulated by the public safety first responders themselves, have grants that are available to meet those needs and then a process in place to be able fairly distribute those funds.

Mr. REICHERT. Out to the people that do the work, right?

Mr. MENCHINI. That is what we do. It has worked well.

Mr. REICHERT. Yes. Absolutely.

Mr. Proctor, did you have one more thing?

Mr. PROCTOR. Just thank you very much—

Mr. REICHERT. You are welcome.

Mr. PROCTOR. —for the opportunity to be here. And if any of us ever had to come back, all you would have to do is call. We would be happy to provide further testimony. We appreciate the highlight of interoperability that Congress is providing, appreciate the support you give us and hope that it will end up in good results out in the field with the folks—

Mr. REICHERT. So do we.

Mr. PROCTOR. —who use it every day.

Mr. REICHERT. Are you free at 5 o'clock? No, I am just kidding.

Members of the committee may have some additional questions for the witnesses, and we will ask you to respond to these in writing. The hearing record will be open for 10 days.

And without objection, the committee now stands adjourned.

[Whereupon, at 3:40 p.m., the subcommittee was adjourned.]

THE STATE OF INTEROPERABLE COMMUNICATIONS: PERSPECTIVES ON FEDERAL COORDINATION OF GRANTS, STANDARDS, AND TECHNOLOGY PART III

Tuesday, April 25, 2006

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON EMERGENCY PREPAREDNESS,
SCIENCE, AND TECHNOLOGY,
Washington, DC.

The subcommittee met, pursuant to call, at 2:13 p.m., in Room 311, Cannon House Office Building, Hon. David Reichert [chairman of the subcommittee] presiding.

Present: Representatives Reichert, Brown-Waite, Pascrell, Harman, Lowey, Norton, and Christensen.

Mr. REICHERT. The Committee on Homeland Security Subcommittee on Emergency Preparedness, Science and Technology will come to order. The subcommittee will hear testimony today on Federal coordination of grants, standards and technology with respect to inter operability and emergency communications. I would first like to welcome our witnesses and thank them for taking time out of their busy schedules to be with us today. I thank you all.

On behalf of the members of the subcommittee, we are glad that you are here today to share your experiences and your knowledge with us. We look forward to hearing your testimony today. This is the final hearing. It is part of series of hearings examining the state of interoperability. Last fall following the devastating loss of communication capabilities as a result of Hurricane Katrina, the Subcommittee on Emergency Preparedness, Science and Technology examined how the operability of communication was the foundation of any interoperable system.

On February 15, 2006, the subcommittee held the second of four hearings dedicated to examining the ongoing challenges of achieving interoperable communications during times of emergency. That hearing analyzed the role and ability of State troopers, fire volunteers, health care facility operators, and managers of critical infrastructure and high risk targets to communicate during times of emergency. Unlike past hearings that focused on the challenges faced by first responders at the scene of an emergency, the third hearing held in March looked at the leadership role of State and local governments in achieving interoperability.

From each witness we heard the same thing. We heard about the need for consistent leadership, for policy makers and government officials to work together more effectively, not for billions of dollars in additional funding.

Today's hearing will feature two panels. The first panel consists of the Federal agencies principally responsible for helping State and local governments achieve interoperable emergency communication capabilities. We want to examine the extent to which these various Federal agencies coordinate their activities and grant programs.

The second panel consists of Federal and nongovernmental entities with expertise in emergency communications standards and technology. Of particular concern is the slow pace of identifying standards.

The government's foremost duty is to safeguard our Nation. When our police officers, firefighters, emergency medical service personnel, public health officials and others charged with safeguarding America are unable to effectively and efficiently interoperate by communicating and coordinating their emergency response, their safety and the lives of those they are aiding are at grave risk. Our Nation has learned the lesson that incompatible emergency communication systems impede intergovernmental coordination efforts. The Federal Government has a long history of addressing Federal, State and local government public safety issues. The important work of government requires many partnerships, including the active participation of private industry, particularly the technology sector, which is why we have an industry representative with us today.

In summation, DHS, Department of Homeland Security, has obligated $2.1 billion to States and local governments thus far to improve interoperability through the purchase of communications equipment and associated projects. In addition, other Federal agencies within the Department of Justice and Commerce, along with the Federal Communications Commission, have made and continue to make significant human and fiscal investments for interoperable emergency communications.

The question before us today is whether our Federal efforts and investments are synchronized and integrated to ensure that the right people have the right information at the right time. So the right decisions are made to protect America. The Chair now recognizes the ranking member, Mr. Pascrell, for his opening statement.

Mr. PASCRELL. Thank you, Mr. Chairman, for holding the fourth and final hearing on the challenges of achieving interoperable communications during times of crisis.

It goes without saying that this is an issue of utmost urgency. I am truly hopeful that this subcommittee, with the leadership of the chairman, will have as its legacy a lasting solution to the communication problems that plague our emergency responders and have plagued them for the last 15 to 20 years. Indeed, we are thus far engaged in a robust exploration on this subject. Speaking extensively to a variety of first responders and State and local government officials, we are all ready for the line, "slowly I turned" when we hear the world interoperability.

Over the recess, I had the opportunity to attend a field hearing and the chairman's district in Washington State, Warden. What we heard from local officials and emergency managers there were the same things I hear daily from safety personnel back in Patterson, New Jersey, that is interoperable communication is critical to defending the homeland and performing everyday public safety services.

The simple fact is this: Lives depend on solving the communications crisis, once and for all. We understand this and we are working towards comprehensive legislation that will truly tackle this problem. That is the purpose and product of our hearings hopefully.

This hearing with its notable witnesses representing the principal Federal agencies responsible for coordinating communication and the communication systems with State and local jurisdictions will no doubt help us as we move forward. Today we must examine whether the Department of Homeland Security is truly acting as the Federal Government's lead agency in coordinating interoperable communication among Federal, State and local governments. We need to probe into the role that various agencies have in assisting the coordination efforts of State and local governments. And we need to identify the Federal Government's strategy for developing a national emergency communications plan.

You know I have been pretty tough on the FCC but the other Federal agencies cannot get their act together in basically enunciating what their goals are, and the FCC cannot do very much for us.

Critical issues—ll of those things are critical—nd issues that have been with us now for too long. It has been said before but it is worth stating repeatedly, when the 9/11 Commission released its final report it found that the inability of our first responders to talk with other each other and their commanders resulted in a loss of life. That is unacceptable and we must all have a sense of urgency about this. This is not a committee assignment or a term paper.

The 9/11 Commission also identified the need for more spectrum as crucial to assist emergency responders in communicating during an emergency such as a terrorist attack or hurricane, and I am convinced that the FCC is now moving in the right direction, Mr. Moran. I would not say that unless I believed it. In 1996, 10 years ago, the Congress asked a blue ribbon committee, the public safety wireless advisory committee, to examine the issue of interoperable communications. And it concluded, that is 10 years ago, that public safety agencies did not have sufficient radio spectrum to do their jobs, but spectrum is not the only impediment to success. As the Department of Homeland Security has concluded, barriers that hinder well coordinated interoperability of efforts are both technical and human. Different jurisdictions may use different equipment, may communicate using different radio frequency bands. There is limited amount of radio spectrum available to public safety. "Funding to replace aging communications equipment is limited, and is subject to jurisdictional budget cycles."

I think that capsulized pretty well what the problem is here. So we have known about the problems. This is 10 years ago. And many have explored the possible remedies that we should under-

take, but while some progress has been made, we are still far from where we need to be.

With this in mind, the President's fiscal year 2007 budget requests no funds for grants to enhance interoperability. The President's fiscal year 2007 budget proposes to eliminate the COPS interoperability grant program, which is charged with awarding technology grants to law enforcement agencies for the purpose of enhancing interoperability and information and sharing.

Is the administration talking out of both sides of its mouth? It is long past the point where we in Washington pay lip service to this problem without actually demanding true results. We are talking about human life. And we talk about these guys and gals, we pat them on the back, we say all nice things about them, but really, we are talking about protecting their lives, helping local agencies protect the lives of people that are on the line every day.

I know my chairman feels the same way that I do, and for that I am grateful. I look forward to continued collaboration with my friend, Chairman Reichert, to help propose serious solutions to serious problems. I want to thank the witnesses for being here today and I look forward for your testimony.

Mr. REICHERT. Thank you, Mr. Pascrell. Other members of the committee are reminded that opening statements may be submitted for the record. We are pleased to have two distinguished panels with us today and we will now call the first panel. And with us today we have the honorable Tracy Henke, Assistant Secretary of Office and Grants and Training, Directorate of Preparedness, U.S. Department of Homeland Security. Dr. David Boyd, director, Office of Interoperability and Compatibility, Directorate of Science and Technology, U.S. Department of Homeland Security. And Mr. John Kneuer was supposed to be here, but unfortunately has a family emergency and could not be with us today.

Next Mr. Kenneth Moran, director, Office of Homeland Security, Federal Communications Commission; and Mr. Carl Peed, executive director, Office of Community Oriented Policing Service, U.S. Department of Justice.

Mr. REICHERT. The Chair now recognizes the Honorable Tracy Henke to testify.

STATEMENT OF HON. TRACY HENKE, ASSISTANT SECRETARY, OFFICE OF GRANTS AND TRAINING, DIRECTORATE OF PREPAREDNESS, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. HENKE. Thank you, Chairman Reichert, Congressman Pascrell and members of the committee. I am pleased to have this opportunity to discuss the efforts of the Department of Homeland Security's Office of Grants and Training to enhance State and local interoperable communications. The Department recognizes the critical importance of interoperable communications in enabling our Nation's public safety personnel to respond quickly, safely, and effectively during an emergency. For this reason, the Office of Grants and Training is working with our partners at the Federal, State, local, territorial, and tribal levels to build interoperable communication capabilities throughout the country.

As you may know, Mr. Chairman, strengthening interoperable communications capabilities is one of seven priorities set by the interim National Preparedness Goal. The Goal is designed to help State and local jurisdictions understand what they need to do in order to be able to respond to a terrorist attack or a natural disaster. At Grants and Training, we have refocused our funding, refocused our training, our exercises and our technical assistance programs to provide the resources State and local leaders need to meet the capabilities and preparedness levels set by the National Preparedness Goal, including interoperable communications.

Today, 43 out of 56 States and territories are working at some level on a Statewide interoperable communications project using G&T funding or technical assistance. However, as you know, Mr. Chairman, we rely on the Department's Science and Technology Directorate to develop interoperable communications standards and to conduct research in this area. Grants and Training's focus is on providing assistance to States to help State and local jurisdictions purchase interoperable communications equipment, develop interoperable communication systems, but I want to stress it is more than just equipment. It is also helping States and local jurisdictions plan, train and exercise. In the past 2 years, we have awarded $2.1 billion in grants for this purpose and developed two major initiatives for which we provided technical expertise and guidance.

Our interoperable communications technical assistance program is working with jurisdictions across the country to help them design and implement interoperable communications systems. Since the program was created in 2003, we have allocated almost $38 million to support what we call the ICTAP and provide assistance to nine States, four territories, and 58 local jurisdictions throughout the Nation. Currently, we are working to respond to requests for assistance from another seven States, one territory and four localities. In addition to the technical assistance provided under ICTAP, we are also working to help major urban areas across the country develop a tactical, interoperable communications plan.

As you know, the 2005 Homeland Security Grant Program required each of the 50 jurisdictions participating in our Urban Areas Security Initiative to develop a plan for providing incident-based critical voice communications among all first responder agencies. States and territories without an urban area specified were required to designate an area to meet this requirement. These plans are due to Grants and Training on May 1st for review and approval.

In addition, in early May, we have invited teams from all approximately 75 participating jurisdictions to Washington to help them plan full-scale exercises to validate their interoperable communication plans and identify gaps in planning, coordination and technology. The teams will use this information to develop an improvement plan that will document the specific steps the region can take to improve communications interoperability. At the same time, the States and localities as well as the Office of Grants and Training and the Department will use the information gained from the exercises and the after action reports to help determine interoperability investments under our Fiscal Year 2007 grant programs. Grants and Training works closely with SAFECOM as well as the

Justice Department, the National Telecommunications and Information Administration at the Department of Commerce and other Federal partners to coordinate our efforts to improve interoperable communications among our Nation's emergency responders.

However, Mr. Chairman, we recognize that there is no silver bullet solution or one-size-fits-all answer to resolving the issues of communications interoperability. Assistance must be tailored to the unique needs and resources of each jurisdiction. For this reason, the Office of Grants and Training will continue to work closely with our partners at the State and local levels, as well as on a national level to ensure that our Nation's first line of home defense, our State and local responders, have the technology, the training and the tools they need to effectively communicate before, during and after a crisis.

Mr. Chairman, thank you, and I am happy to answer questions at the appropriate time.

Mr. REICHERT. Thank you.

[The statement of Ms. Henke follows:]

PREPARED STATEMENT OF HON. TRACY A. HENKE

APRIL 25, 2006

Chairman Reichert, Congressman Pascrell, and Members of the Subcommittee, I am Tracy Henke, and I serve as the Assistant Secretary of the Office of Grants and Training (G&T) within the Preparedness Directorate of the Department of Homeland Security (DHS). It is my pleasure to appear before you today to discuss the current status of the Department's efforts to enhance state and local interoperable communications, and our coordination internal and external to the Department of Homeland Security.

I wanted to thank the Members of the Committee for your ongoing support of the Department. I also thank you, Mr. Chairman, for your foresight and leadership on the issue of interoperable communications, which is a cornerstone of our ability to save lives and protect property during threatened or actual emergencies and disasters including terrorist events.

Mr. Chairman, G&T is an essential element of the Department's capacity building efforts at the state, local, territorial, and tribal levels to deter, prevent, respond, and recover from emergencies and disasters of all kinds, including terrorism. DHS, through G&T, 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.

G&T and its predecessor organization has provided assistance to all 50 States, the District of Columbia, the Commonwealth of Puerto Rico, and the U.S. territories. Through our programs and initiatives, more than 1.4 million emergency responders from more than 5,000 jurisdictions have been trained and conducted more than 500 exercises. By the end of Fiscal Year (FY) 2006, states and localities will have received from DHS over $17.9 billion in assistance and direct support since September 11, 2001. This includes specifically $2.1 billion in grant assistance that states and local jurisdictions have obligated thus far to improve interoperability through the purchase of communications equipment and other projects.

The Department's three primary sources of financial assistance to states and local communities, the State Homeland Security Program (SHSP), Law Enforcement Terrorism Prevention Program, and the Urban Area Security Initiative (UASI), require states and urban areas to assess their risk, capabilities, and needs, 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. While financial assistance is an important tool with which we support our state and local partners, the Department offers a wide array of support through technical assistance, training and exercise programs.

INTEROPERABLE COMMUNICATIONS A PRIORITY UNDER HSPD–8

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 the Department of Homeland Security, 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.

Through the work that is being conducted under HSPD–8, the Department has developed an Interim National Preparedness Goal that establishes 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 is producing 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. The National Preparedness Goal focuses on seven national priorities, including "Strengthening Interoperable Communications Capabilities." This priority is meant to achieve interoperability not only in terms of communications, but also in the broad ability of systems and organizations to provide service and to accept service from one another across jurisdiction lines, enabling them to operate effectively together.

It should be noted as well that two recent Hurricane Katrina reports—one from Congress and the other from the White House—both mention the enhancement of public safety communications interoperability as a critical National priority. The Department is working to enhance Nationwide communications interoperability through a number of different programs and initiatives. I would like to take this opportunity to discuss these initiatives with the Subcommittee.

INTEROPERABLE COMMUNICATIONS TECHNICAL ASSISTANCE PROGRAM (ICTAP)

In the area specific to my direction, G&T administers more than three dozen technical assistance programs. One of our most important technical assistance efforts to date is the Interoperable Communications Technical Assistance Program (ICTAP). ICTAP is designed to enhance interoperable communications among local, state, and Federal emergency responders and public safety officials, and is associated with the UASI grant program. The goal of the ICTAP program is to enable local public safety agencies to communicate as they prevent or respond to a weapons of mass destruction 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. This program enables the jurisdictions to understand the scope of their interoperability needs, and implement solutions to address those needs.

ICTAP has received requests for assistance from 46 of the Department's 50 UASI partners, as well as 9 States and 5 U.S. Territories. In the past 4 years, $37.9 million has been made available for ICTAP's efforts. All requests for ICTAP assistance are coordinated through the states to ensure consistency with state, and, where applicable, the urban area homeland security strategies. ICTAP provides technical assistance at no cost to jurisdictions in conjunction with the implementation of state and UASI preparedness 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. The current listing of the states, regions and territories in which we are working is attached to my testimony in Appendix A.

While the ICTAP program has provided significant assistance and support to a number of urban areas and states, it is 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 and coordination with the key communication stakeholders in that region.

TACTICAL INTEROPERABLE COMMUNICATION PLANS

As part of the FY 2005 Homeland Security Grant Program (HSGP) each of the Department's 50 UASI partners was required to develop a Tactical Interoperable Communications Plan (TICP). States and territories that did not have a designated urban area were required through grant guidance to designate a multi-jurisdictional metropolitan area or region as a substitute. There are now a total of 75 urban areas and multi-jurisdictional metropolitan areas that are required to submit a TICP. This

initiative builds on an effort led by SAFECOM and G&T in FY 2004 called RapidCom that focused on achieving tactical-level emergency interoperable communications in ten major urban areas. States are required to submit the TICPs to G&T by May 1, 2006, for review and approval.

Tactical interoperable communications is defined as the rapid provision of on-scene, incident based mission critical voice communications among first-responder agencies (EMS, fire, and law enforcement), as appropriate for the incident, and in support of incident command system as defined in the National Incident Management System (NIMS). Each TICP has six critical elements:

(1) Urban Area Information—A basic description of the urban/metropolitan area and its efforts to address interoperable communications. A list off all agencies represented in the TICP including those agencies represented in the Urban Area Working Group

(2) Governance Structure—An overview of the governance structure including the contact information for the members of the governing body

(3) Interoperable Equipment—A detailed listing of all interoperable communication equipment available in the urban/metropolitan area

(4) Policies and Procedures—Specific information on how urban/metropolitan areas will utilize their communications equipment and adhere to proper protocol

(5) Incident response plan—A detailed listing of functional disciplines to which the TICP applies, and plans for how the available interoperable communications equipment will be used within the NIMS structure to support the response to the incident.

(6) Training—Information on the progress and future plans to ensure that adequate staff are training as communications unit leaders as defined by NIMS

The objective is for each Urban Area to have plan that will allow them to achieve command level interoperability within one hour of the incident. Within 6 months of submitting their TICPs, G&T will provide, if requested, direct assistance to the 75 identified areas to validate the plans by conducting a full scale exercise. The exercise will be evaluated by a team of subject matter experts and will utilize exercise evaluation guidelines that are consistent with previously identified target capabilities to improve interoperable communications. At the conclusion of the exercise, an after action report (AAR) for each of the 75 identified areas will be created to clearly present any issues the public safety community must address, including recommendations to achieve meaningful communication interoperability. Included in the AAR, as an appendix, will be an improvement plan that will document specific steps the region can take to improve their interoperability. Meanwhile, the Science and Technology Directorate Office of Interoperability and Compatibility is in the process of conducting a Nationwide Baseline Survey to measure the capabilities necessary for first responder agencies to achieve communications interoperability. Through the TICP exercise, the subsequent AAR process, and Nationwide Baseline Survey, the Department can identify shortfalls, and work with our state and local partners to fill communication gaps and focus resources for where they are needed the most to improve communication interoperability. This effort should drive state's FY 2007 investments related to interoperability.

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. We work hard to closely coordinate these efforts.

SAFECOM

The Department is well aware of the importance of developing national interoperability policy. For guidance on these issues, G&T relies on SAFECOM, which is the Federal government's umbrella office for coordination of public safety interoperability programs, to provide standards and conduct research that can help our jurisdictions develop a better interoperable communications program. As an example, all FY 2006 guidance for G&T grant programs that provide eligibility for spending on communications interoperability requires compliance with the SAFECOM grant guidance on interoperability. 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, we have entered into a Memorandum of Agreement with SAFECOM to codify the areas in which we can work more effectively to-

gether. This includes continuation of grant support for SAFECOM projects like the Statewide Communication Interoperable Planning methodology, as well as coordinating other areas of mutual interest such as the dissemination of grant guidance and providing technical assistance in the field. SAFECOM has also recently allocated resources to support the development and subsequent exercise validation of the TICP. SAFECOM will soon distribute a national survey to assess the baseline communications capabilities of thousands of state and local public safety agencies. We look forward to combining these results with the results of the TICP process to gain a more detailed picture of interoperability capabilities.

NIMS Integration Center

The NIMS is a nationwide approach for all levels of government to work effectively and efficiently together to prepare for and respond to domestic incidents. Together with SAFECOM, the NIMS Integration Center (NIC) is currently developing the Communications Unit Leader (COML) training course referenced in FY 05 HSGP Guidance for the TICP. ICTAP assisted the NIC in developing the core competencies for the COML that will be used as part of the certification requirements. When completed, the COML will be integrated into existing DHS training programs.

INTERAGENCY COORDINATION

Federal Interagency Coordination Council (FICC)

G&T, is represented on the Federal Interagency Coordination Council (FICC) addressing interoperability. 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.

Coordination with the Department of Justice

In coordinating with the Department of Justice (DOJ) on interoperability initiatives, the Department through G&T has ensured that response agencies have incorporated this work into their homeland security interoperability efforts. For example, ICTAP has worked closely with personnel from DOJ's Integrated Wireless Network, Wireless Management Office—25 Cities Program, National Institute of Justice-CommTech Program, and Community Oriented Policing Services (COPS)—Interoperable Communications Technology Program to ensure that ongoing Federal efforts are closely coordinated.

Federal Partnership for Interoperable Communications (FPIC)

We also participate in Federal Partnership for Interoperable Communications (FPIC) meetings. FPIC's goal is to foster partnerships among Federal agencies that promote the exchange of knowledge and resources among members of the wireless communications community. This participation assists in the creation and maintenance of a Federal roadmap to achieve wireless communications interoperability across Federal departments, bureaus, and agencies.

National Telecommunications and Information Administration

The National Telecommunications and Information Administration (NTIA), located within the Department of Commerce, received a significant source of funding for interoperable communications grants to states and localities through the Deficit Reduction Act of 2005 (Public Law 109–171). Under provisions of the bill, the Assistant Secretary of NTIA is authorized to use $1 billion from the Digital Television Transition and Public Safety Fund to carry out a grant program to assist public safety agencies in the acquisition of, deployment of, or training for the use of interoperable communications systems that utilize, or enable interoperability with systems that can utilize, reallocated public safety spectrum for radio communications. The Department of Homeland Security is working closely with NTIA to ensure that any grants provided under this program are consistent with the approach taken by G&T and the SAFECOM initiatives. Further, DHS is committed to working with NTIA to ensure that these funds are spent in a manner that will have a meaningful impact on the state of communications interoperability.

CONCLUSION

In closing, thank you for convening this hearing on the vital issue of communications interoperability. The Department of Homeland Security is committed to working with Congress and our stakeholders to continue to address this critical area of need. It is a cornerstone effort to enhancing our Nation's preparedness. Mr. Chairman, let me reinforce the Department of Homeland Security's continuing commitment to support the Nation's state, local, tribal, and territorial partners to ensure that America's emergency responders have the ability to effectively communicate before, during, and after a crisis. This concludes my prepared statement. I am happy

to respond to any questions that you and the members of the Committee may have. Thank you.

Appendix A: States and UASI Sites Receiving Support Under the Interoperable Communications Technical Assistance Programs

Active UASI ICTAP Sites		Pending UASI ICTAP Sites	ICTAP States	ICTAP U.S. Territories
Anaheim, CA	Orlando, FL	Long Beach, CA	California	Guam
Atlanta, GA	Philadelphia, PA	Alabama	Connecticut	Northern Mariana Islands
Baton Rouge, LA	Phoenix, AZ	Baltimore, MD	Hawaii	Puerto Rico
Buffalo, NY	Pittsburg, PA	South Carolina	Idaho	Virgin Islands
Charlotte, NC	Portland, OR	Iowa	Kentucky	
Chicago, IL	San Antonio, TX	Utah	Louisiana	
Cincinnati, OH	San Diego, CA	Montana	New York	
Cleveland, OH	San Francisco, CA	Wyoming	New Jersey	
Columbus, OH	San Jose, CA	Boston, MA	Washington	
Dallas/Ft. Worth/ Arlington, TX	Santa Ana, CA	Rhode Island		
Denver, CO	Seattle, WA	Sacramento, CA		
Detroit, MI	St. Louis, MO	American Samoa		
Fresno, CA	Tampa, FL			
Honolulu, HI	Toledo, OH			
Houston, TX	Twin Cities, MN			
Indianapolis, IN	Washington, DC			
Jacksonville, FL	Alaska			
Kansas City, MO	Arkansas			
Las Vegas, NV	Delaware			
Los Angeles, CA	Kansas			
Louisville, KY	Maine			
Miami, FL	Mississippi			
Milwaukee, WI	North Dakota			
New Haven, CT	New Hampshire			
New Orleans, LA	New Mexico			
New York City, NY	South Dakota			
Oakland, CA	Tennessee			

Appendix A: States and UASI Sites Receiving Support Under the Interoperable Communications Technical Assistance Programs—Continued

Active UASI ICTAP Sites		Pending UASI ICTAP Sites	ICTAP States	ICTAP U.S. Territories
Oklahoma City, OK	Vermont			
Omaha, NE	West Virginia.			

Mr. REICHERT. The Chair recognizes Dr. Boyd.

STATEMENT OF DAVID BOYD, DIRECTOR, OFFICE OF INTEROPERABILITY AND COMPATIBILITY, DIRECTORATE OF PREPAREDNESS, DHS

Mr. BOYD. Good afternoon, Chairman Reichert, Ranking Member Pascrell, and members of the subcommittee. I want to thank you for inviting me to speak to you today.

As the events of September 11 and Hurricanes Katrina and Rita demonstrated, interoperability is not possible when the foundation for operations has been degraded or destroyed.

The White House report on Hurricane Katrina said it plainly. "The complete devastation of the communications infrastructure in the gulf region left responders without a reliable network to use for coordinating emergency response operations." Secretary Chertoff has made this issue a top priority for the Department.

SAFECOM, the Presidential management initiative, established to strengthen and coordinate interoperability initiatives at all levels of government, has created highly successful tools and methodologies to achieve interoperability and initiated and coordinated communications research and development initiatives across the Federal Government. These tools support all the technical, policy and best practices elements required to achieve interoperability.

While I am pleased to report that we have made significant progress on many fronts, I want to be clear that moving the Nation's 60,000 public safety agencies toward wireless interoperability is an enormous undertaking. Much remains to be done at all levels of government if we are to be successful. SAFECOM grant guidance, for example, is required by OMB to be included in every Federal grant program that may support communications investments. The guidance identifies the requirements that must exist before Federal funds can be spent on equipment procurement and brings clarity to grant recipients regarding how to best build, maintain, upgrade and operate communications systems to promote interoperability. In the 15 years, before SAFECOM undertook the coordination of standards for interoperability, only one standard in the P25 suite of eight had been created. Under SAFECOM leadership and funding and with the collaboration of the National Institute of Standards and Technology, and the support of both industry and our public safety partners, we dramatically accelerated this process, completing at least three additional standards just since last October.

Products incorporating these standards should be available in about a year, but I want to emphasize that standards cannot, by

themselves, achieve interoperability. It is possible however, as we demonstrated in RapidCom 1, that command level emergency interoperability can be achieved, even in the absence of comprehensive standards in any community willing to commit to SAFECOM guidelines. In accordance with the Intelligence Reform and Terrorism Prevention Act of 2004, SAFECOM took its statewide communications interoperability planning guide, the SCIP, first piloted with the State of Virginia, and initiated two additional regional communications pilots, one in Nevada and one in Kentucky, to create locally-driven plans for improving public safety communications. At the same time, we worked to better integrate the urban areas of Las Vegas, Nevada and Louisville, Kentucky into their respective statewide plans. These initiatives are producing comprehensive communications and interoperability plans that will provide a viable framework for a unified multi-jurisdictional response to high consequence events.

This effort has yielded essential tools and best practices that will be applied by localities and will States on a national level. In fact, the city of Louisville will put Kentucky's interoperability plan to the test in its preparations for the May 6 Kentucky Derby.

SAFECOM also continues to work with the National Governors Association, the National League of Cities, the U.S. Conference of Mayors, the National Association of Counties, and similar organizations that can function as a force multiplier for wireless interoperability.

The National Governors Associations Policy Academy, for example, worked last year with five States to introduce SAFECOM tools and methodologies to their interoperability planning and will expand this efforts to include additional sites this year. Several more SAFECOM tools and resources will be delivered in the coming months, including a request for a proposal RFP tool, to help agencies write proposals that ensure they get what they need and ensure that what they get is compatible with SAFECOM's national guidance, guidance to help jurisdictions test and evaluate plans, procedures and equipment in preparing for an all-hazard incident. This tabletop methodology originally employed in RapidCom 1 is being enhanced for use in RapidCom 2 with the Office of Grants and Training, a national baseline study to provide the first ever quantitative assessment of the Nation's level of interoperability and continued funding and coordination of research and development initiatives into new technologies, such as software-defined radio, IP, and cognitive radio initiatives already underway in defense, DHS, NIST, and others.

More SAFECOM activities and accomplishments can be found in my statement for the record and in the SAFECOM toolkits which we provided to each of your offices as well as on the SAFECOM Web site.

The SAFECOM strategy is built on an understanding that achieving both operability and interoperability, among the Nation's public safety agencies is a national, not just a Federal effort. I would be happy to answer any questions you may have.

Mr. REICHERT. Thank you.

[The statement of Boyd follows:]

FOR THE RECORD

PREPARED STATEMENT OF DR. DAVID BOYD

TUESDAY, APRIL 25, 2006

Introduction

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

When I appeared before this committee late last year, I testified that SAFECOM [1] is the federal program dedicated to improving the connectivity of the 60,000 public safety agencies through interoperable wireless communications. With this program, we are working to enable public safety agencies to communicate across jurisdictions and disciplines during a disaster to ensure a coordinated response to save lives.

Today's testimony will focus on the state of interoperable communications and what S&T is doing to improve communications and interoperability across the nation. Specifically, the testimony will address S&T's interoperability initiatives and the formidable challenges that are inherent in moving the nation's public safety community towards wireless interoperability.

In discussing interoperability, I must be clear about the relationship between operability and interoperability. Simply put, operability must be in place for interoperability to be possible. Operability exists when responders have a basic level of communications. Once that is established, interoperability—defined as the ability for public safety agencies to talk to one another via radio communications systems to exchange voice and/or data with one another on demand, in real time, when needed, regardless of specific spectrum or technology—becomes possible.

Operability, or lack thereof, played a key role in the recent natural disasters of 2005. While people may assume that public safety agencies are already interoperable, these recent disasters tell a different story. Too many emergency responders still cannot talk to parts of their own organizations, let alone communicate with agencies in neighboring cities, counties, or states, during a crisis. As September 11, 2001 and Hurricanes Katrina and Rita demonstrated, interoperability is not possible when the foundation for operations has been degraded or destroyed. It is essential that operability remain a focus point.

The White House report on Hurricane Katrina released in February said it plainly: "The complete devastation of the communications infrastructure [in the Gulf region] left responders without a reliable network to use for coordinating emergency response operations." [2] Because operability is the foundation of interoperability, Secretary Chertoff has made this issue one of the Department's highest priorities. In a recent speech he pointed out that "in addition to interoperability, you have to have operability. If all of the communications have been blown down, if the satellite phones are running out of power, if all the radio towers are down, then it's not a question of interoperability, it's a question of ability to operate at all." [3]

Evidence indicates that operability cannot be ensured in austere conditions in many of the nation's 60,000 public safety agencies. We must make a concerted effort to remove the obstacles that are preventing these agencies from achieving basic operability. While most public safety agencies have some basic level of communication, operability remains an issue of concern, as it must be in place before interoperability becomes possible. Toward this end, SAFECOM has made significant progress in overcoming some of the most common barriers to operability in emergency incidents by providing guidance for achieving operability and by addressing issues associated with system migration and the coordination of communications spectrum policy. Tools which SAFECOM has developed that address operability include the coordinated grant guidance and the Statement of Requirements (SoR). SAFECOM will soon conduct the National Interoperability Baseline survey to determine the level of operability and interoperability across the nation. SAFECOM will also leverage the Office of Grants and Training's (G&T) Communications Assets Survey and Mapping tool, which inventories infrastructure information, to help determine the level of public safety operability in the nation today.

---

[1] SAFECOM is a communications program of the Office for Interoperability and Compatibility (OIC), managed by the Office of Systems Engineering and Development in the Science and Technology Directorate of the Department of Homeland Security (DHS). SAFECOM provides research, development, testing and evaluation, guidance, tools, and templates on communications-related issues to local, tribal, state, and federal public safety agencies.

[2] White House, *Federal Response to Hurricane Katrina: Lesson Learned* (2006) pg. 37.

[3] Remarks by Secretary Michael Chertoff to the International Association of Fire Fighters Legislative Conference March 21, 2006.

It is important to remember that facilitating operability and interoperability between and among the nation's public safety agencies requires a national rather than a Federal effort. It requires public safety practitioners at all levels of government and across the nation to work collaboratively to develop a better appreciation of the steps they must take to achieve operability and interoperability and of the tools and resources that are available through SAFECOM that will help them along the way.

To address the most urgent interoperability needs, however, SAFECOM is working with its Federal partners [4] to develop and implement a national strategy that ensures that all public safety agencies have the necessary tools and resources to meet the immediate demands for interoperability to meet the most likely emergencies, and to support the migration from their existing communications capabilities to more interoperable systems.

I want to provide an overview of the components—the tools and initiatives—that SAFECOM is using to help local and state public safety agencies accelerate their communications progress *now,* but I also want to make clear that while we are making significant progress on a number fronts, much more remains to be done.

Impact on Interoperable Communications

Operational Support

One major SAFECOM effort is focused on assisting local and state agencies in the development of interoperable communications plans. While SAFECOM recognizes that each locality and state may have different communications needs and requirements, the effective implementation of consistent criteria in each plan provides a common foundation for establishing an interoperable system. SAFECOM, therefore, provides guidance, tools, and coordination in support of these local and state needs. To this end, SAFECOM is working with G&T to leverage resources to provide funding and technical assistance. The following sections describe SAFECOM initiatives that focus on near-term local, statewide, and/or regional interoperable communications support.

RapidCom

In 2004, SAFECOM, in coordination with G&T, took steps to improve interoperability in 10 top-threat cities through the Urban Area Security Initiative (UASI). RapidCom 1 helped the targeted areas achieve interoperable communications between incident commanders within one hour of an event. This effort incorporated tabletop exercises, planning support, tool development, training, and technology operating procedures to ensure better communications among top-level officials in each city. SAFECOM published a report on lessons learned from RapidCom 1 to assist states and localities in their effort to implement a system of interoperable communications. To continue this initiative, $5 million was appropriated to S&T's Office for Interoperability and Compatibility (OIC) to expand RapidCom in FY 2006.

The Interoperability Continuum (see fig. 1), is an example of one of the tools that supported the RapidCom initiative. It allows public safety agencies to assess progress in key areas affecting interoperability such as governance, standard operating procedures, technology, training and exercises, and usage. The Interoperability Continuum is designed to illustrate how communications interoperability is a complex goal, requiring multiple simultaneous improvements in communications use, governance, standard operating procedures, technology, and training/exercises. The degree of interoperability depends upon the improvement of all five of these factors—no one factor (e.g. technology) is the solution to obtaining interoperability. For this reason, OIC and G&T have invested considerable resources into developing standards, providing technical assistance to state and local entities, and facilitating regional coordination and standard operating procedures. Communications continues to be one of the largest uses of G&T grant funds by states and urban areas—to date, nearly $2.2 billion has been spent for interoperable communications since September 11, 2001.

[4] SAFECOM's partners are listed in Appendix A.

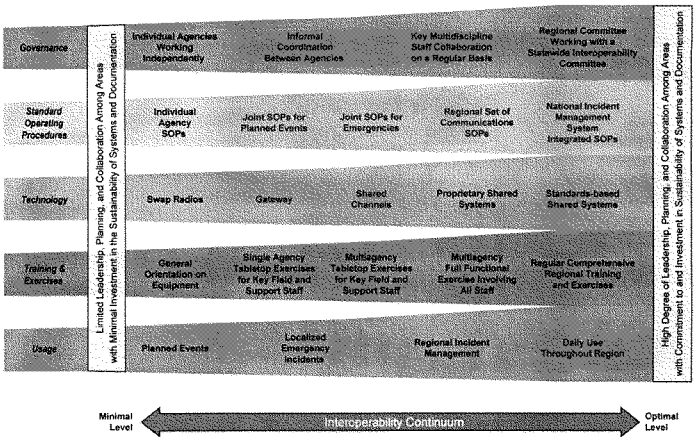


Figure 1: Interoperability Continuum

We have worked with G&T to accelerate the development of Tactical Interoperable Communication Plans (TICP)[5] – through RapidCom 2 – in 77 high-threat regions, including all past and present UASI regions. G&T is encouraging prioritization of grant funds for this effort, and is providing technical assistance through their TICPs. G&T expects to receive more specific plans in May, and will be working with each region to conduct exercises that test these interoperability plans.

Statewide Communications Interoperability Planning
In 2004, SAFECOM developed the Statewide Communications Interoperability Planning (SCIP) Methodology to help state-level officials create a statewide interoperability plan. Working with the Commonwealth of Virginia, SAFECOM developed this approach to guide statewide planning efforts in areas such as choosing local stakeholders, addressing relevant issues, and developing and implementing plans in a manner that is consistent with that of other states.

The SCIP serves as a basis for much of SAFECOM's local and state work, and its guidance has resulted in a successful statewide planning initiative in Virginia, and more recently the SCIP methodology served as the basis for the Regional Communications Interoperability Pilots (RCIP) in the State of Nevada and the Commonwealth of Kentucky. In all three states, appropriate

[5] All Urban Areas and select other metropolitan areas are required as part of the FY 2005 Homeland Security Grant Program to develop and validate a Tactical Interoperable Communications Plan (TICP). The goal of the plan is to enable rapid on-scene, incident-based mission critical voice communications among all emergency responder agencies as they prevent or respond to a Chemical, Biological, Radiological/Nuclear, and Explosive (CBRNE) terrorist attack. The TICP leverages other local, state, and Federal interoperability efforts whenever possible to enhance the overall capacity for agencies and individuals to communicate with one another.

emergency response agencies at both local and state levels have been directly involved in the planning efforts. As a result, state leadership has succeeded in designing systems that are in line with the diverse needs of their public safety stakeholders. The Policy Academies of the National Governors Association's Center for Best Practices also use the SCIP to help improve statewide interoperable communications in Georgia, Idaho, Louisiana, Nevada, and Wisconsin. These states now have a roadmap based on a locally-driven, bottom-up approach to planning for improving communications systems. The SCIP methodology is posted on SAFECOM's Web site.

According to Chris Essid, Virginia's Commonwealth Interoperability Coordinator within the Office of the Secretary of Public Safety, "Virginia now has a Strategic Plan for Statewide Communications Interoperability that was developed by local public safety responders for local public safety responders."[6]

As SAFECOM works to strengthen local and state initiatives to develop interoperable communications plans, it has made significant progress in addressing a requirement of the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108–458). In its work with Nevada and Kentucky on the RCIP projects, SAFECOM ensured that state and local coordination remained a priority in the states' efforts to develop interoperable communications plans. Input from emergency responders and policy makers from all levels of government has been incorporated into the RCIP to provide the most comprehensive plan for Nevada and Kentucky.

The impact of SAFECOM's work reaches beyond Nevada and Kentucky and across the nation. By leveraging the lessons learned, best practices, and subsequent templates, SAFECOM is able to provide jurisdictions nationwide with the tools to successfully initiate planning processes based on sound, practitioner-driven input. The guidance has also been promulgated through G&T. As a pre-condition for interoperability funding in next year's (FY2007) Homeland Security Grants, states will be required to submit interoperability strategies consistent with the SCIP methodology. Work in both Nevada and Kentucky is nearing completion and a final report to Congress will be delivered in June 2006.

Coordinated Grant Guidance

Historically, different sources of funding have brought different interoperability requirements. This lack of coordination has led to stove-piped systems, incoherent planning processes, and incompatible communications goals. One of SAFECOM's early successes in working with G&T, as well as other agencies in the Federal government (e.g., the Office of Community Oriented Policing Services in the Department of Justice) was the creation of coordinated and consistent criteria for agencies receiving federal funds to use in guiding their grantees. This criteria, or grant guidance, lists the planning requirements that must be followed before federal funds can be spent on equipment procurement. It also provides specific questions that should be addressed in grant applications to ensure that the potential recipients of federal funds have thoroughly assessed how their money will improve interoperability. At the direction of the Office of Management and Budget, this grant guidance is now required for all public safety grant programs that provide Federal funds for communications interoperability.

The grant guidance maximizes the effectiveness for the significant resources available for public safety communications. Nearly $2.2 billion has been allocated for public safety interoperability under this guidance, which also provides succinct criteria to grant recipients as to how to best build, maintain, upgrade, and operate communications systems to promote interoperability. Coordinated grant guidance also results in a more responsive Federal funding system for the creation of national communications interoperability. SAFECOM's grant guidance is updated at the beginning of each fiscal year to accommodate any changes in technologies, standards, or other conditions that might affect the public safety community.

Tool Development

As depicted in the Interoperability Continuum (see fig. 1), public safety agencies need to integrate and coordinate many issues to achieve interoperable communications. The following tools help agencies move along the lanes of the Continuum.

SAFECOM is developing a Request for Proposal (RFP) tool that will radically simplify the often cumbersome local and state procurement processes and ensure compatibility with SAFECOM's national strategy. Through SAFECOM's work with localities and states, the program has seen confusion among localities and states in terms of what information to include in an RFP. This tool will be a step-by-step,

[6] Statewide Communications Interoperability Planning (SCIP) Methodology, November 2004 http://www.safecomprogram.gov/NR/rdonlyres/9628BE4B–E7A5–4F1B–9179–2CFCF2653CA9/0/SCIPMethodology.pdf

how-to guidebook for writing the major RFPs needed for communications interoperability planning and implementation. It will guide state and local public safety officials through the complex process for procuring communications systems and equipment and services for enhancing interoperability capabilities. Specifically, the guide will demonstrate best practices for identifying needs, determine the appropriate method of procurement, develop an RFP, write a statement of work, evaluate proposals, and follow federal guidance, requirements, and standards for communications interoperability. The RFP tool is currently under development and will be released in the coming months.

While the SCIP streamlines planning, and the RFP tool enhances communications equipment procurements, attention must also be paid to providing consistent guidance regarding multi-jurisdictional exercises concerning plans and equipment purchases. It is critical to enable jurisdictions to test and evaluate the plans and procedures that they have developed in preparing for an all-hazard incident. Therefore, SAFECOM and our partners at G&T are developing consistent training practices and a communications-specific tabletop methodology. SAFECOM expects this methodology to help communications departments identify and discuss gaps in current capabilities and processes and to recognize differences in capabilities. It is intended to guide communities and Federal technical assistance programs in planning, designing, and executing communications exercises for public safety. Communities may modify and apply the methodology to suit specific needs, realities, and cultures in the local area. The content, including the lessons learned and recommendations presented, are based directly on input from local first responders who participated in exercise planning, design, and execution. This tabletop methodology builds on the methodology employed in RapidCom 1 and is being finalized now.

National Interoperability Baseline Initiative

To date, there is no quantitative or qualitative assessment of the nation's level of interoperability. A baseline is crucial to assess the maturity of operational, governance, and technical considerations for interoperable communications; identify capability gaps; and direct Federal investments as well as future SAFECOM initiatives. Later this year, SAFECOM will administer a National Interoperability Baseline survey to 23,000 public safety agencies to measure the current state of interoperable communications capabilities across the nation. The results of the survey will provide the first quantitative assessment of public safety's interoperable communications capabilities.

SAFECOM will conduct a second assessment as a follow-up to the National Interoperability Baseline. This assessment will continue to measure the state of interoperable communications capabilities across the nation and allow SAFECOM to pilot more tools and methods. The results of the survey will provide a comparable quantitative assessment of public safety's interoperable communications capabilities to show improvement compared to the original baseline.

The RFP tool, the tabletop methodology, and the baseline will all help local, tribal, state, and federal public safety agencies to proceed along the lanes of the Interoperability Continuum toward a more optimal level of interoperability.

Technology Guidance

Just as the tools and efforts described above are directly mapped to progress along the Interoperability Continuum, so too is the work SAFECOM has done to advance communications technology. While technology is not the only component of a system of systems approach for improving interoperable communications, it remains an essential piece.

Project 25 Standards

Project 25 (P25) is a suite of eight standards that will enable any component of one communications system to work with components of another communications system. These eight technical standards are intended to provide public safety access to non-proprietary, open architecture standards. What this means to emergency responders is that they could take their P25-compliant portable radio and travel across the country in response to a disaster and communicate within another jurisdiction's P25 system. These standards for equipment are essential to achieving communications interoperability and will enable emergency responders using equipment from different manufacturers to communicate with one another.

While SAFECOM promotes the completion and deployment of the P25 suite of standards, it is important to note that P25 is only one set of standards. There are instances in which communities have achieved interoperability through non-P25 solutions. In fact, there are instances where requiring P25 might actually be irrelevant (for example, if the equipment being purchased has to work with non-P25 equipment, such as the case with some analog equipment frequently used by the

fire services), or where moving to a P25 system without adequate planning and coordination might damage existing interoperability. Additionally, we understand that, as technology changes, other standards might become more appropriate.

Currently, SAFECOM is working with the National Institute of Standards and Technology (NIST) to support the public safety community and industry in their efforts to accelerate the development of the P25 suite of standards for interoperable communications. In the fifteen years before SAFECOM undertook this coordination, only one standard in the suite of eight had been created. Since NIST and SAFECOM have partnered with industry and public safety to accelerate P25, significant progress has been made. Three standards have been completed including the Inter-RF Subsystem Interface, the Fixed/Base Station Subsystem Interface, and the Console Subsystem Interface. The public safety community can expect technology resulting from these three standards to be available next year.

SAFECOM is continuing to work with NIST to complete the remaining four interfaces of the P25 suite of standards. By continuing to use the voluntary consensus standards process, it is likely that the remaining interfaces will be completed in the next few years, but it will take the cooperation of both industry and practitioner members of the standards process to make this happen.

With input from the user community, P25 standards have been developed to allow for backward compatibility with existing digital and analog systems and to provide for interoperability in future systems. New and old equipment will be able to work together. This will allow public safety agencies to maintain interoperability with other agencies as they begin to replace and upgrade their current communications systems. For example, agencies that purchase new P25 compatible equipment ideally will be able to operate that equipment within its existing communications infrastructure.

To ensure that P25 standards will be implemented where appropriate, they will be tied to SAFECOM's grant guidance. SAFECOM's investment in this standards activity will result in public safety being better enabled to swap or share communications equipment when responding to emergencies.

SAFECOM is also working with G&T to link standards to interoperable communications planning efforts. Localities and states will be encouraged to use P25 equipment where it makes sense. Standards are already being tied to grants and will be included in the Tactical Interoperable Communications Plans.

P25 Compliance Assessment Program

Public safety demands that equipment claiming to be P25 compliant—or generally capable of its manufacturer's claims—will communicate with other P25 radios. Unfortunately this is not often the case. Initial testing shows that often one manufacturer's "P25-compliant radio" will not communicate with another manufacturers "P25-compliant radio." SAFECOM is currently addressing this issue by developing a P25 conformance testing program in partnership with NIST to ensure equipment really does meet the new P25 standards. NIST, in cooperation with technical representatives from the Institute for Telecommunication Sciences and industry representatives, has established a framework for the program and is moving into the first stage of testing. The safety of emergency responders will be enhanced when industry's claims of P25 compliance can be measured objectively and independently. This initiative will also ensure federal grant dollars are being used appropriately to purchase equipment that is truly P25 compliant.

Statement of Requirements

It became clear in 2003 that a comprehensive understanding of public safety communications requirements was needed before any advanced research or development was likely to succeed. As a result, in 2004 SAFECOM produced version 1.0 of the Statement of Requirements for Public Safety Wireless Communications and Interoperability (SoR). Developed with public safety practitioner input, the SoR defines operational and functional requirements for public safety communications. Later this year, SAFECOM will release version 1.1, which further defines user requirements to enable industry to develop equipment that meets the needs of public safety and federal users. Additionally, SoR version 1.1 presents unified technical requirements for interoperable communications and enables results-oriented discussions between public safety, industry and policy makers. SAFECOM is also developing version 2.0 of the SoR which will begin to incorporate quantitative values for the requirements. Version 2.0 will quantify the requirements for the most important applications identified by the public safety community: mission-critical voice, and emerging technologies for tactical video. Version 2.0 will also help industry to develop equipment that meets the new public safety requirements. Version 2.0 will be published later this year.

Public Safety Architecture Framework

Having established a set of requirements, SAFECOM began building a national architecture framework. SAFECOM is now completing the development of a Public Safety Architecture Framework (PSAF) that, with the SoR, will serve as a tool to help the nation's public safety community understand the technical requirements and system modernization plans without imposing requirements that stifle innovation. The PSAF will be released later this month.

In moving public safety towards greater interoperability, the impact of the PSAF is likely to be substantial. Currently, public safety has no effective way of comparing systems and existing communications infrastructure, which prevents them from identifying paths towards interoperability. The PSAF, for the first time, will enable local, state, and federal agencies to analyze current systems and determine what is necessary to achieve interoperability with other systems and agencies. The PSAF also inventories and identifies capability gaps to help public safety agencies target areas for improved interoperability.

Working with Industry

Seamless national interoperability depends upon the development and implementation of solutions based on public safety's expressed needs. The SAFECOM program works with the public safety community and industry as equipment is developed and included in local and state planning efforts across the nation. On March 23, 2006, S&T hosted the inaugural SAFECOM Industry Summit in Washington, DC. The Industry Summit afforded SAFECOM and the public safety community a valuable opportunity to engage with the telecommunications industry on critical interoperability issues. The summit addressed public safety's role in the SAFECOM program, the impact of standards on new technologies, and how to leverage SAFECOM's technical and procedural foundations to optimize research, development, testing, and evaluation efforts. More than 300 attendees from the telecommunications industry participated in the event, which according to Charles Werner, Fire Chief, Charlottesville, Virginia "established a firm foundation from which public and private partnerships may now build upon."

Conclusion

SAFECOM is developing high-quality tools and resources *today* to help public safety migrate towards an interoperable system-of-systems nationwide. Although it is difficult to predict a specific date when full interoperability will be achieved, SAFECOM has created the roadmap and is developing the tools to help agencies move along it. The Interoperability Continuum, the SoR, and the PSAF among others will enable public safety and industry to ensure further interoperability. As you are aware, interoperability saves lives; those of our public safety officials and the citizens they serve. Though many challenges remain, DHS is committed to ensuring that the nation's public safety community has the necessary tools and resources to ensure communications systems are interoperable when they must be. However, the Federal government cannot fix interoperability alone. Both public safety and industry must be committed to using and improving the available tools and models to make sound investments while addressing all of the critical elements of interoperability.

In closing, I want to thank you for your past support and I ask for your continued support. I appreciate the opportunity to testify before you today. I would be pleased to answer any questions you may have.

Appendix A: Table of Federal Partners

Federal Partner	Mission Area	Coordination
Department of Commerce National Institute of Standards and Technology (NIST).	• Development and promotion of standards and technology to enhance communications interoperability.	• Coordination on the acceleration of P25 standards • P25 compliance testing program • Ongoing collaboration on industry and technology development

Appendix A: Table of Federal Partners—Continued

Federal Partner	Mission Area	Coordination
Department of Commerce National Telecommunications and Information Association (NTIA).	• The Executive Branch's primary voice on domestic and international telecommunications and information technology issues within the Department of Commerce. • Performs spectrum management for all Federal agencies.	• SAFECOM grant guidance • Regular coordination and collaboration on communications activities • SAFECOM Emergency Response Council representation • Member of the Federal Partners for Interoperable Communications (FPIC)
Department of Defense (DoD) Joint Tactical Radio System (JTRS).	• Communications across the U.S. military.	• SAFECOM Emergency Response Council representation
Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA).	• Provides on the ground operational support in response to all-hazards disasters.	• Coordination with the National Incident Management System Integration Center on Communications Unit Leader Training curriculum and other communications activities
DHS/ Department of Treasury/Department of Justice (DOJ) Integrated Wireless Network (IWN).	• Communications among federal users.	• Regular coordination and collaboration on communications activities
DHS National Communications System (NCS).	• Consortium of Federal departments and agencies that have assets, resources, requirements and/or regulatory authority regarding national security and emergency preparedness (NS/EP) communications. • Responsible for the Federal Telecommunications Standards Program.	• Collaboration on DHS communications activities
DHS Office of Grants and Training.	• Block grants to state and locals • Technical assistance to state and locals.	• SAFECOM grant guidance • RapidCom 1 and 2 • Table-top exercises • SAFECOM Emergency Response Council representation
DHS Wireless Management Office (WMO).	• Communications among DHS users.	• Collaboration on DHS communications activities • Spectrum Plan Advisory Committee • Participation in working groups • SAFECOM Executive Committee (EC) and Emergency Response Council representation • Coordination on IRTPA report on telecommunications needs
DOJ High-Risk Metropolitan Area Interoperability Assistance Project ("25 Cities")	• Connectivity between federal and local users.	• RapidCom • Table-top exercises • SAFECOM EC representation

Appendix A: Table of Federal Partners—Continued

Federal Partner	Mission Area	Coordination
DOJ Community Oriented Policing Services (COPS).	• Discretionary grants to state and locals.	• SAFECOM grant guidance • Peer review and grantee training programs in FY 2004 • SAFECOM Emergency Response Council representation
DOJ CommTech Program	• Technical assistance to state and locals. • Research and development	• SoR development • RapidCom 1 • SCIP • Table-top exercises • SAFECOM Emergency Response Council representation
Federal Communications Commission (FCC).	• Regulates interstate and international communications by radio, television, wire, satellite and cable. • Responsible for all spectrum issues associated with public safety.	• Spectrum Needs Assessment • Narrowbanding Report to Congress • SAFECOM Emergency Response Council representation
National Guard Bureau (NGB).	• Communications across the National Guard.	• SAFECOM Emergency Response Council representation • SAFECOM representation on NGB Senior Advisory Board

Appendix B: Other S&T Directorate Efforts Regarding Standards Development and Interoperability

The S&T Standards Portfolio partners with private sector American National Standards Institute (ANSI) and other DHS components and federal agencies on standards for emergency preparedness and response

Standards Portfolio has worked with the private sector to establish a public-private partnership for homeland security standards development. The ANSI Homeland Security Standards Panel (HSSP) has a proactive agenda for sponsoring workshops and conferences in emergency preparedness. The chart below lists some of these activities. As a direct result of the meetings in New York City from January—March 2004, the 9/11 Commission was informed about National Fire Protection Association (NFPA) 1600: Standard for Emergency Preparedness and Business Continuity which had been developed with strong participation from the Federal Emergency Management Agency (FEMA). Subsequently, Secretary Ridge testified before the 9/11 Commission that DHS was adopting NFPA 1600 (action by Standards Portfolio) and the DHS Office of the Private Sector co-sponsored with NFPA a series of regional workshops on emergency preparedness.

ANSI–HSSP Workshop Activities on Emergency Preparedness and Training

Subject	Dates	Location
Workshop on Private Sector Emergency Preparedness and Business Continuity (with the 9/11 Commission).	January 28, 2004	NYC
Workshop on Private Sector Emergency Preparedness and Business Continuity (with the 9/11 Commission).	February 27, 2004	NYC
Workshop on Private Sector Emergency Preparedness and Business Continuity (with the 9/11 Commission).	March 22, 2004	NYC

ANSI–HSSP Workshop Activities on Emergency Preparedness and Training—Continued

Subject	Dates	Location
Workshop on Training Program Standardization for First Response to WMD Events.	June 10, 2004	Braintree, MA
Workshop on Training Program Standardization for First Response to WMD Events.	September 23, 2004	Arlington, VA
Workshop on Training Program Standardization for First Response to WMD Events.	January 27, 2005	Arlington, VA
Workshop on Citizen Preparedness (in conjunction with workshop on emergency communications).	December 2, 2004	Schaumburg, IL
ISO International Workshop Agreement (IWA) Meeting on Emergency Preparedness.	April 24–26, 2006	Florence, Italy
Workshop on Lessons Learned from Hurricane Katrina and Role for Standards and Conformity Assessment Programs.	May 2006	NYC (tentative)
Fifth ANSI–HSSP Plenary Meeting (emergency preparedness is the proposed theme for the event).	October 2006	NYC or Gaithersburg, MD

Standards Portfolio: Cooperation with DHS Office of Grants and Training

The S&T Standards Portfolio has created a framework for standards development, adoption and advice to DHS Office of Grants and Training (G&T) to guide purchases of equipment with $3.9 billion in grants to states and localities. Management Directives were developed and approved by the Under Secretary for Management which governs the operation of seventeen standards working groups that are shepherding standards for specific threats and conventional mission needs. This includes a key step that allows S&T technical reports and studies to be converted to grants guidance by G&T. This handshake between RDT&E and grants guidance is critical to technology transfer for all S&T mission elements.

Standards and G&T are working collaboratively to develop a model for providing G&T with standards for equipment, standard operating procedures, and training for state and local entities. Our main contacts in G&T are with the System Support Division. Their three main activities are: 1) the SAVER program for test and evaluation of commercial-off-the-shelf equipment; 2) the Center for Domestic Preparedness (CDP) in Anniston, AL that trains 50,000 emergency responders annually on equipment and procedures for responding to terrorists' incidents; and 3) the Memorial Institute for the Prevention of Terrorism (MIPT) Responder Knowledge Base (www.RKB.mipt.org) for advising responders on equipment and standards.

G&T has assigned a Standards Coordinator who attends weekly staff meetings with the Standards Portfolio as well as all Standards Working Groups and brings additional subject matter experts to working group meetings. Working with this coordinator and the three programs listed above, the Standards Portfolio is coordinating with System Assessment and Validation for Emergency Responders (SAVER) and CDP on developing standards for chemical, biological, radiological and explosives detectors. With this effort, we will ensure that training protocols are developed for new equipment as it is developed by S&T.

We have also greatly expanded the materials available on the Responder Knowledge Base by supplying information on standards and product comparisons. Direct collaborations on standards for testing and evaluation include: sampling, testing and training for suspicious biological materials, and testing and evaluation for blast resistant trash receptacles. We are also working with the G&T Training and Exercises Division to provide standard training protocols that can be incorporated in G&T training and exercises programs. We are working to include subject matter experts from S&T as guest instructors in training and exercises programs in G&T, and conversely, to include G&T experts in all S&T Integrated Process Teams (IPT) related to standards, equipment and training.

The Nation's First Radiation Detector Standards

The S&T Standards Portfolio has worked with other federal agencies (Department of Defense (DOD), Defense Threat Reduction Agency, Department of Energy) and DHS components, including the offices of Research & Development and Systems Engineering and Development's Counter-Measures Test Bed, Customs and Border Patrol, the Secret Service, Transportation Safety Administration, and more recently Domestic Nuclear Detection Office) to develop and adopt standards for radiation detectors for use by emergency responders. These standards were developed in a record 15 months by IEEE/ANSI N42. Standards Portfolio sponsored testing against these standards at NIST and four national laboratories (S&T Office of Research and Development (ORD) project management) and results of these tests were made available to DHS Grants and Training for publication on their Web site (Responder Knowledge Base). These results were shared with Domestic Nuclear Detection Office and the other federal agencies. This radiation detector Commercial Off-Of-The-Shelf (COTS) testing and evaluation study focused attention on the G&T data base, and they expanded access to the data base to other federal agencies due to increased interest in their website.

Standards for Local Response to Suspicious Powders

The Standards Portfolio is leading an interagency effort to develop standards for biological detectors used by emergency responders to suspicious powder events. Other agencies involved include DOD, U.S. Department of Health and Human Services (HHS) Food and Drug Administration and Centers for Disease Control (CDC)/ National Institute for Occupational Safety and Health (NIOSH), Environmental Protection Agency, U.S. Department of Agriculture, and the Federal Bureau of Investigation (FBI) Hazardous Materials Response Unit (HMRU). The working group was co-chaired by Office of Science and Technology Policy. DHS components included in this standards working group include G&T Center for Domestic Preparedness and the Bio-Countermeasures Portfolio in S&T. This project resulted in performance standards for hand-held assays for *Bacillus anthrax.* The work also indicated a need for standard operating procedures, sampling standards and training standards for responding to suspicious powders. This is an excellent example of the value of gathering all the stakeholders (DHS, FBI, HHS/CDC and HazMat teams—represented by the NFPA) to define the operational goals for national standards that are used by voluntary private sector organizations—but still meet the needs of diverse federal agencies.

Protective Equipment Standards for Emergency Responders

The Standards Portfolio has led the national effort to develop Personal Protective and Operational Equipment for emergency responders and all this work is closely coordinated with DHS G&T, FEMA and the U.S. Fire Administration. The portfolio has worked with an interagency team that includes NIST, DOD (Edgewood and Natick) and HHS (CDC/NIOSH). Other DHS components included in the planning process are the S&T Emergency Preparedness and Response Portfolio, Homeland Security Advanced Research Projects Agency, and WMD Operations as well as Coast Guard R&D Center. This work has led to development and adoption of three NIOSH and five NFPA standards for respirators and protective ensembles. Work is underway with American Society for Testing and Materials on standards for Urban Search and Rescue (USAR) robots which includes a team assembled from 20 FEMA USAR task forces.

Mr. REICHERT. The Chair recognize Mr. Moran.

STATEMENT OF KENNETH MORAN, DIRECTOR, OFFICE OF HOMELAND SECURITY, FEDERAL COMMUNICATIONS COMMISSION

Mr. MORAN. Thank you. Good afternoon, Mr. Chairman and distinguished members of the subcommittee. My name is Ken Moran, and I serve as the director of the Federal Communications Commission, Office of Homeland Security. In my testimony today, I will provide an update of the Commission's actions in the areas of interoperable communications and emergency communications preparedness since I last appeared before the subcommittee last October.

Pursuant to the Intelligence Reform and Terrorism Act, the Commission conducted an assessment of short-term and long-term spec-

trum needs for emergency response providers and submitted a report to Congress regarding that assessment in December. The report reached the following principle conclusions: Mobile broadband communications implemented in combination with upgraded equipment and associated training and close coordination can offer emergency response providers emergency important capabilities. Emergency response providers would benefit from the development of an integrated interoperable nationwide network capable of delivering broadband services throughout the country.

While commercial wireless technologies are not appropriate for every type of public safety communication, there is a place for commercial providers to assist public safety in securing and protecting the homeland. While the effort to address the short term spectrum needs of public safety is underway, attaining a wholesale assessment of long-term spectrum needs is an ongoing task. The Commission is also working to solve the interference problems in the 800 megahertz band by tightening the interference standards and by reconfiguring the band to separate the public safety systems from the commercial systems.

Reconfiguration of the 800 megahertz band is currently taking place on a region-by-region basis. When completed, the reconfiguration will alleviate the interference problems in the 800 band. Moreover, approximately 4.5 megahertz of additional spectrum will be made available for public safety communications systems. In light of the findings set forth in the report to Congress, last month the commission started a rule making to examine the operational, technical and spectrum requirements for meeting Federal, State, and local public safety communications needs through the year 2010.

At the urging of the public safety community and in recognition of the need for spectrum appropriate for broadband communications, the Commission seeks comment on whether certain channels in the 700 megahertz public safety bands should be modified to accommodate broadband communications.

In addition, the Commission adopted rules requiring providers of digital broadcast and cable TV, satellite radio, and direct broadcast satellite services to participate in the Commission's emergency alert system. The Commission also initiated a rule seeking comment on how the Commission can expedite the development of next generation alert warning systems that take full advantage of digital media's potential.

In January, the Commission established an independent panel to review the impact of Hurricane Katrina on communication networks. The Katrina panel is studying the impact of Hurricane Katrina on all sectors of telecommunications and media, including public safety communication, reviewing the sufficiency and effectiveness of infrastructure recovery efforts, and making recommendations regarding ways to improve disaster preparedness, network reliability and communications among first responders. Several representatives from the public safety sector, including law enforcement, fire, and emergency medical on are on the panel. The panel will report its findings and its recommendations to the Commission in June.

Finally, in March, the Commission voted to create a new public safety and homeland security bureau. The Commission proposes to

take functions currently residing in seven separate bureaus and offices at the Commission and consolidate them into one bureau. By creating a unified structure to oversee and respond to public safety and homeland security matters, the Commission seeks to improve its operating efficiency and effectiveness in areas it deems of highest priority.

In addition, the new structure will enable the Commission to better coordinate its national security, homeland security, public safety and emergency communications roles.

In conclusion, the Commission is committed to working with its Federal, State, tribal and local partners, with industry and with the Congress to ensure public safety communications are as reliable as possible and are fully interoperable and that effective emergency plans and assets are at the ready to quickly restore these services if they ever fail. I would be pleased to answer questions. Thank you.

Mr. REICHERT. Thank you, Mr. Moran.

[The statement of Mr. Moran follows:]

PREPARED STATEMENT OF KENNETH P. MORAN

APRIL 25, 2006

Good morning, Mr. Chairman and distinguished members of the Subcommittee. My name is Ken Moran and I serve as the Director of the Federal Communications Commission's Office of Homeland Security in the Commission's Enforcement Bureau. In that role, I am primarily responsible for the national security, homeland security, and emergency preparedness responsibilities of the Commission.

The Commission's strategic goal for homeland security is to provide leadership in evaluating and strengthening the nation's communications infrastructure, in ensuring rapid restoration of that infrastructure in the event of disruption, and in ensuring that essential public health and safety personnel have effective communications services available to them at all times, and particularly in the event of an emergency. Interoperability is an essential aspect of ensuring effective communications. First responders must have the ability to communicate seamlessly, especially during a disaster.

In my testimony today, I will provide an update of the Commission's recent activities in the area of interoperable communications and emergency communications preparedness. Since I last appeared before the Subcommittee in October, the Commission has:

- Submitted a Report to the Congress, pursuant to the Intelligence Reform and Terrorism Act, regarding the development of an interoperable nationwide network and on the use of commercial wireless technologies for public safety communications;
- Continued the transition of commercial wireless and public safety services within the 800 MHz spectrum;
- Initiated a rulemaking proceeding to examine allocation of the 24 MHz spectrum that will be available for public safety communications when the DTV transition is completed;
- Issued rules extending the reach of the emergency alert system to include digital broadcast and cable TV, digital audio broadcasting, satellite radio, and direct broadcast satellite services;
- Solicited comments on how the Commission can best help develop a next-generation alert and warning system that takes full advantage of digital media's potential;
- Established a federal advisory committee, known as the Katrina Panel on Communications Networks, that is developing recommendations for improved emergency preparedness and response for future disasters; and
- Proposed the establishment of a new bureau, the Public Safety and Homeland Security Bureau, which will be the unified entity for carrying out the Commission's public safety, homeland security, national security, and emergency communications responsibilities.

Briefly, I will provide detail on each of these activities:

Report to Congress

Pursuant to the Intelligence Reform and Terrorism Act, Congress asked the Commission, in consultation with DHS and NTIA, to undertake a study and prepare a report assessing the short-term and long-term spectrum needs of emergency response providers. The Commission conducted the assessment and submitted the report to Congress in December, 2005. The report addressed not only the questions posed by Congress, but also considered the many thoughtful proposals submitted in the record for addressing the spectrum needs of traditional public safety entities and other critical emergency response providers, as well as some lessons learned from the impact of hurricanes Katrina, Rita, and Wilma on our nation's communications infrastructure. The report reached the following principal findings:

- Emergency response providers would benefit from the development of an integrated, interoperable nationwide network capable of delivering broadband services throughout the country.
- While commercial wireless technologies are not appropriate for every type of public safety communication, there is a place for commercial providers to assist public safety in securing and protecting the homeland.
- While the effort to address the short-term spectrum needs of public safety is underway, attaining a wholesale assessment of long-term spectrum needs is an ongoing task.
- Mobile, broadband communications, implemented in combination with upgraded equipment, associated training and close coordination, could offer emergency response providers many important capabilities. To this end, and at the urging of public safety community, the Commission will expeditiously examine whether certain channels within the current allocation of twenty-four megahertz of public safety spectrum in the 700 MHz band could be modified to accommodate broadband communications.

800 MHz

As you are aware, the public safety community has experienced interference problems in the 800 MHz band. In 2004, the Commission provided a two-pronged solution to the problem. First, the Commission adopted a plan to reconfigure the 800 MHz band to separate public safety and critical infrastructure industry entities from commercial wireless carriers, such as Nextel. Second, the Commission adopted a specific technical standard regarding what constitutes unacceptable interference to public safety and critical infrastructure providers. The Commission will hold commercial carriers strictly responsible for complying with this standard.

Reconfiguration of the 800 MHz band is taking place on a region-by-region basis based upon the 55 National Public Safety Planning Advisor Committee (NPSPAC) regions. Each of the 55 NPSPAC regions is assigned to one of four staggered "prioritization" waves. Band reconfiguration for non-NPSPAC channels began last year. In February, band reconfiguration for NPSPAC channels began.

The reconfiguration will alleviate the interference problems that public safety communications systems have faced in the 800 MHz band from commercial wireless systems. Moreover, an average of 4.5 megahertz of additional spectrum in the 800 MHz band will be made available for public safety communications systems.

700 MHz

In light of the findings set forth in the Report to Congress, last month the Commission started a rulemaking proceeding to examine the operational, technical, and spectrum requirements for meeting federal, state and local public safety communication needs through the year 2010. The Commission believes that mobile broadband communications can offer public safety many important capabilities, including delivery of real-time video, images, automated dispatch, multi-media alerts and real-time monitoring. Accordingly, accommodating public safety's need for mobile, broadband communications may be critical in the long-term. Certain public safety entities have identified the 700 MHz band as a potential home for broadband operations. At the urging of the public safety community, and in recognition of the need for spectrum appropriate for broadband communications, the notice seeks comment on whether certain channels within the current twenty-four megahertz of public safety spectrum in the 700 MHz public safety band (764-776 MHz and 794–806 MHz), should be modified to accommodate broadband communications. The Commission is using this proceeding to implement many of the recommendations of the National Coordination Committee (chartered by the Commission to formulate standards for interoperable voice and data systems in the recently-allocated 700 MHz public safety band), which

are designed to ensure total, mandatory voice interoperability between all radios used in the 700 MHz band.

Emergency Alert System (EAS)

On November 3, 2005, the Commission adopted rules requiring providers of digital broadcast and cable TV, digital audio broadcasting, satellite radio, and direct broadcast satellite services to participate in the Commission's EAS program. With the exception of DBS service, all affected entities must comply with these new requirements by December 31, 2006. DBS services must comply no later than May 31, 2007.

Also on November 3, the Commission initiated a rulemaking seeking comment on how the Commission can expedite the development of a next-generation alert and warning system that takes full advantage of digital media's potential. Questions included what type of architecture would support a next-generation system and what common protocols would be required to allow an alert to be delivered simultaneously to multiple platforms such as radios, televisions and wireless devices. The Commission also asked how it could facilitate the effective integration of wireless technologies into a next generation alert and warning system, and whether traditional telephone companies that plan to provide high definition digital content to customers' homes should have public alert and warning responsibilities. In addition, the Commission asked how a next generation EAS can more effectively reach individuals with hearing and vision disabilities and non-English speaking individuals. Finally, the Commission sought comment on how the Commission should coordinate its efforts with FEMA and how, if at all, the participation of state and local authorities in the EAS system should be changed. The record in this proceeding closed on February 23, 2006.

Katrina Panel

In January, the Commission established the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks (Katrina Panel) pursuant to the Federal Advisory Committee Act. Specifically, the Katrina Panel is: studying the impact of Hurricane Katrina on all sectors of the telecommunications and media industries, including public safety communications; reviewing the sufficiency and effectiveness of the recovery effort with respect to the infrastructure; and making recommendations regarding ways to improve disaster preparedness, network reliability, and communication among first responders.

The Panel's membership includes several representatives from the public safety sector, including law enforcement, fire fighters, and emergency medical services. Also serving on the Panel are representatives from all segments of the communications industry including the wireline, wireless, satellite, broadcast, and cable industries. The Panel established three working groups: (1) Infrastructure Resiliency; (2) Recovery Procedures and Coordination; and (3) Emergency Communications. Thus far, it has held three meetings. The Panel has heard testimony about the impact of Hurricane Katrina from representatives of public safety agencies, telecommunications carriers, broadcasters, satellite radio service providers, equipment manufacturers, consultants and consumer organizations. In addition it has seen presentations from federal officials and Panel members regarding emergency communications problems and solutions.

The Panel will report its findings and recommendations to the Commission by June 15, 2006. The Commission looks forward to the Panel's report and plans to carefully consider all of its recommendations.

Reorganization

On March 17, 2006, the Commission unanimously voted to create a new Public Safety and Homeland Security Bureau. The action is subject to Congressional notification. The Commission proposes to take functions currently residing in seven separate Bureaus and Offices at the Commission and consolidate them into one Bureau.

This Bureau will provide a single central hub for the development of policies and rules to promote reliable communications for public safety, national security, and disaster management. The Bureau will be tasked to expend all of its resources to make sure that the Commission does its part to support reliable emergency communications and address the needs of first responders, law enforcement, and emergency response personnel.

The new Bureau will be organized along three functional lines: Policy, Public Communications Outreach & Operations, and Communications Systems Analysis. It will be responsible for all Commission policy, outreach, and operations with respect to public safety communications, including 911 and Enhanced 911 (E911) requirements, Public Safety Answering Points (PSAPs), operability and interoperability of public safety communications, and matters falling under the Communications Assistance for Law Enforcement Act (known as CALEA). Setting the requirements for priority emergency communications, such as the Telecommunications Service Priority (TSP) and Wireless Priority Service programs that the National Communications System (NCS) administers, along with the national Emergency Alert System (EAS), network security and reliability, and communications infrastructure protection will also be a responsibility of the new Bureau. In addition, the new Bureau's Policy Division will handle the licensing of spectrum for public safety entities, a task that currently resides in the Commission's Wireless Telecommunications Bureau.

The Commission's other public safety and homeland security responsibilities will also fall within the new Bureau's jurisdiction. These responsibilities include Continuity of Government Operations (COG); Continuity of Operations (COOP); the Commission's 24 hour a day, 7 day a week Communications and Crisis Management Center; disaster management coordination and outreach; Federal Advisory Committee coordination (e.g., Media Security and Reliability Council (MSRC) and the Network Reliability and Interoperability Council (NRIC)); and industry information collection and attendant analytical activities.

By creating a unified structure to oversee and respond to public safety and homeland security matters, the Commission seeks to improve its operating efficiency and effectiveness in areas it deems of highest priority. In addition, the new structure will enable the Commission to better coordinate its national security, homeland security, public safety, and emergency communications roles with its federal partners as well as with state, tribal, and local governments, and industry.

Other Activities

In addition to the activities described above, the Commission continues to work closely with federal agencies and national public safety organizations, including:

- DHS/SAFECOM/FCC–WTB Interoperability Working Group
- SAFECOM Executive Committee and Advisory Committee Working Groups
- NTIA Ad Hoc 214 Working Group (a committee established by the Interdepartmental Radio Advisory Committee (IRAC) with responsibility for, among other things, reducing regulatory barriers to better facilitate interoperability between federal agencies and their state and local counterparts)
- Public Safety Regional Planning Colloquiums
- National Public Safety Telecommunications Council

Conclusion

The importance of effective public safety communications cannot be over-stated, especially during disasters, when the American public is most vulnerable. The Commission is committed to working with its federal, state, tribal and local partners, and with the Congress to ensure these communications systems are as reliable as possible, are fully interoperable, and that effective emergency plans and assets are at the ready to quickly restore these services if they ever fail. I would be pleased to respond to your questions.

Mr. REICHERT. The Chair now recognizes Mr. Peed, and I must say that I am pleased to see Carl again. I worked with Carl when I was the sheriff in Seattle and was fortunate enough back at that time when the COPS office had some funding that was coming its way to be the benefactor of some of the money that was coming through the COPS office. So thank you Carl for your help and for your service. Good to see you again.

STATEMENT OF CARL PEED, EXECUTIVE DIRECTOR, OFFICE OF COMMUNITY ORIENTED POLICING SERVICES (COPS) U.S. DEPARTMENT OF JUSTICE

Mr. PEED. Thank you, Chairman Reichert and Ranking Member Pascrell, and members of the committee. Thank you for the oppor-

tunity to address you here today. I am pleased to appear before you on behalf of the Office of Community Oriented Policing Services, or COPS. As a 25-year veteran of law enforcement, I am proud to lead an organization whose mission is to support local efforts to reduce crime through community policing. This is why COPS has worked to establish and successfully administer our interoperability communications technology grant program, which is the very program that I am here to speak to you about today.

Communications interoperability refers to the ability to share information across disciplines, in jurisdictions near radio and data networks on demand, in real-time, when needed and as authorized to do so.

The interoperability projects, funded by the COPS office, represent region specific approaches to enhancing interoperability and improving the capacity of emergency service personnel to connect to broader, multi-regional systems. To date, COPS invested more than $242 million to support real-time information sharing and enhanced command and control capacity by first responders in 63 of the Nation's metropolitan areas in 37 States and one territory.

In fiscal year 2003, COPS awarded $66.5 million to 14 communities to develop interoperable communications networks. In 2004, COPS awarded $82.6 million in grants to 23 communities. And in 2005, COPS awarded 26 agencies nearly $93 million through this program. This year, COPS has appropriated $10 million to continue the interoperable communications technology grant program. We plan to use these funds to make several grants and to support training, technical assistance and publications that will assist the field in our ongoing efforts to improve interoperability.

There are general elements of the way we have made these grants that I want to bring to your attention today. First is the degree with which we coordinated with out other fellow entities and the kind of partnerships we engaged in. COPS recognized early in 2003 that it would be critical that we have strong relationships with other Federal agencies and departments, the professional associations that represent State and local law enforcement and technical experts and first responders like firefighters.

The COPS office had experience with efficient grant management. We had a strong relationship with law enforcement and had awarded many grants for purchasing and employing crime fighting technology. But we recognize that in the complicated and dynamic world of interoperable communications, the COPS office needed to form new collaborative partnerships and coordinate with other Federal agencies. Within the Department of Justice, we coordinated with the Office of Justice Programs, the National Chief of Justice, and the Bureau of Justice Assistance, with the Department of Justice's high risk metropolitan areas interoperability project or the 25 cities project, and within the Department of Homeland Security with SAFECOM, the Office For Interoperability and Compatibility, the Office of Grants and Training, which was formerly the Office of Domestic Preparedness and Federal Emergency Management Agency.

In Commerce, we are coordinating with the National Institute of Standards and Training. We have also worked closely with the International Associations of Chiefs of Police, the National Sheriffs

Associations, the National Organization of Black Law Enforcement Executives, the Police Executive Research Forum Representing Law Enforcement, as well as APCO, the Association of Public Safety Communications, and the International Association of Fire Chiefs. They helped us design and implement this program.

Second, COPS designed a grant system that allowed us to take advantage of many of these partnerships in the form of a peer review panel to evaluate grant proposals. Using the relationship we have with some of my fellow panelists here today, SAFECOM and DHS and representatives of local law enforcement to effectively review the proposals and on the Federal level, to ensure the highest degree of consistency with existing interoperability standards. The panel of peer reviewers was comprised of law enforcement, fire and emergency medical service personnel as well as technological professionals, so each provided an expert evaluation on the practical and technical aspects of the proposals.

Finally, we invested heavily in providing training and technical assistance opportunities for the grantees. We recognize there is a need to provide ongoing support to grantees as they further develop these networks. Therefore, we offer a wide array of training and technical assistance resources. We have hosted technical assistance kick-off conferences, assisting grantees with everything from handling the administrative requirements of the grant, to addressing interjurisdictional liability issues related to interoperable networks, and we have hosted advanced technical assistance workshops, a national interoperability summit, and we have offered on-site remote technical assistance and worked closely with our partners, especially SAFECOM, to produce a "how to" publication that will provide unified Federal voice to jurisdictions looking for interoperability guidance.

Let me share an example from the program with you. In Texas, the city of Austin, which is in Travis County, will use COPS funds to expand their existing 800 megahertz regional radio system into neighboring Williamston County, and to upgrade Williamston County older analogue system so it is compatible with Austin's. Once this project is completed, it can be used as a Statewide benchmark that will enable State, local and Federal agents to communicate on a common platform.

America has learned that tragedies, natural disasters and crimes do not recognize jurisdictional boards. My neighbor's problem is my problem. Like we learned from the terrorist attacks on 9/11 at the World Trade Center and the Pentagon, the D.C. sniper attacks and Hurricane Katrina, when we act together, we are stronger than when we attempt to go it alone.

First responders have accepted the challenge of achieving interoperability, and COPS is pleased to have been a partner with many Federal agencies in a coordinated Federal response to address this need.

Thanks in part to these grants, police and fire communications and information systems will be developed in the future with an eye toward interoperability. In closing, Mr. Chairman, thank you for the opportunity to speak to you today, and I will be happy to answer any questions.

[The statement of Mr. Peed follows:]

PREPARED STATEMENT OF CARL R. PEED

APRIL 25, 2006

Good Afternoon. I am pleased to appear before you today on behalf of the Department of Justice's Office of Community Oriented Policing Services (COPS). As a twenty-five year veteran of law enforcement, I am proud to lead an organization whose mission is to support local efforts to reduce crime through community policing.

In 1994, Congress passed the Violent Crime Control and Law Enforcement Act, which created the Office of Community Oriented Policing Services (COPS) and our mission of advancing community policing and assisting state, local, and tribal law enforcement throughout the country. Since then, more than two-thirds of the nation's law enforcement agencies have received assistance from COPS programs, including training and technical assistance, grants for purchasing and deploying crime fighting technology, and law enforcement hiring assistance.

Community policing calls for law enforcement agencies to develop collaborative relationships within the community that support a detailed understanding of community needs, community norms, and ultimately, community vulnerabilities. Furthermore, community policing encourages law enforcement to rely on this understanding of the community to implement proactive measures that prevent crime and illegal behavior before it evolves into a significant criminal or terrorist act, and to effectively respond to emergencies and disasters.

We have heard repeatedly from local law enforcement that the nexus between national efforts to secure our homeland from terrorism and disaster and local efforts to secure individual communities from all types of threats and emergencies is clear. This is why COPS has worked in close cooperation with the Department of Homeland Security in administering the Interoperable Communications Technology Grant Program, which is the program that I am here to speak with you about today.

One of the major issues currently facing emergency service providers is the inability of first responders to share vital information during crisis, and our interoperability grant program directly addresses this issue. Communications interoperability refers to the ability to share information across disciplines and jurisdictions via radio and data networks on demand, in real-time, when needed, and as authorized.

Effective emergency response requires operational coordination and the sharing of vital information among numerous public safety agencies. Unfortunately, many emergency service providers rely on communication systems developed solely to meet their own unique needs, and these systems are often not compatible with those of neighboring agencies.

Recognizing this challenge, Congress, through the Omnibus FY 2003 Appropriation and the Wartime Supplemental Appropriation, allocated $66 million to COPS to administer a discretionary interoperability program for law enforcement agencies.

During the same fiscal year, the Emergency Preparedness and Response Directorate (i.e. FEMA) in the Department of Homeland Security (DHS), received almost $80 million for a similar program aimed at various public safety agencies. Therefore, we worked together, and with the assistance of the Department's National Institute of Justice (NIJ) and the Department of Commerce's National Institutes of Standards and Technology (NIST), COPS and FEMA developed a coordinated program for FY 2003.

Since the Interoperable Communication Technology Program's inception, COPS has worked closely with the NIJ and the Justice Department's Bureau of Justice Assistance, the our 25 city High Risk Metropolitan Areas Interoperability Project, the DHS Office for Interoperability and Compatibility—SAFECOM, DHS' Office of Grants and Training, FEMA, and the NITJ. We have collaborated with these entities on issues such as establishing program guidelines and criteria, reviewing applications, developing national interoperable standards, and providing interoperable training and technical assistance to first responders.

In fact, these partnerships are a key contributor to the success of federal efforts. COPS recognized early on that Government-wide goals would best be achieved by collaborating with other federal agencies, technical experts, and experienced practitioners. An integral part of implementing successful interoperable networks is the willingness and capacity of the systems' users to work together effectively. For COPS to overlook the very actions that we require of grant recipients would be hypocritical.

Our collaborative efforts were even acknowledged in the FY 2005 Appropriations Conference Report. In the language of the Report, "the Conferees commend the COPS Office for its coordination with other federal agencies that deal with public safety interoperability. The Conferees believe coordination of federal efforts is crit-

ical to ensure our nation's safety and a necessity if we are not to fall victim to the pitfalls of the past."

With a program of this nature we believed it was imperative to leverage the program's funds to ensure the greatest possible impact on the largest population centers in the country. This was COPS' goal when inviting jurisdictions to apply from the beginning. Initially, in 2003, we invited the largest 50 metropolitan statistical areas (MSA) in the United States and the largest metropolitan area in each State to apply for the program. In 2004, we received additional guidance from Congress instructing us to consider both large and small entities. Therefore, we used the same process, and invited the two largest MSAs in each State to apply. In 2005, the process was the same, but due to increased funding we added the three largest MSAs in each State. Ultimately, by increasing the number of MSAs in each State that were eligible to apply, and as previous grantees were removed from the list of potential applicants each year, we steadily increased the number of smaller jurisdictions that became eligible to benefit from the program.

In fiscal year 2003, COPS awarded $66.5 million to 14 communities to develop interoperable communication networks. In fiscal year 2004, COPS awarded $82.6 million in grants to 23 communities in 17 states, and in fiscal year 2005, COPS awarded 26 agencies nearly $93 million through this program. In total, this equates to more than $242 million to support real-time information sharing and enhanced command and control capacity by law enforcement in 63 of the nation's largest metropolitan areas.

The grants provided one year of funding (three years in 2005), and population determined the amount of funding available to grantees. The maximum federal share for a grant award is $6 million for MSA regions with a population of greater than 500,000 persons according to the 2000 Census, and $3 million for MSAs with a population of 500,000 persons or less. The program requires a local cash match of 25% of the total project cost.

Successful applications for the program demonstrate a detailed understanding of the first responder interoperability needs within the MSA applying for funds. Proposals have also been required to be comprehensive and convey a clear and demonstrated plan for achieving improved multi-jurisdictional and/or multi-disciplinary interoperability.

Again, COPS recognized the importance of partnerships, and we worked closely with SAFECOM and our other partners during the proposal evaluation process. We relied on partnerships to effectively review the proposals, and on the federal level to ensure the highest degree of consistency with existing interoperability standards.

All applications were peer reviewed to ensure that the best proposals were funded. The panel of peer reviewers was comprised of law enforcement, fire, and emergency medical service personnel, as well as technological professionals who provided expert evaluation on the technical aspects of the proposals.

The major factors considered during the peer review process have been: (1) the quality and merit of applications, which represents 40% of the application score; (2) projected project outcomes and deliverables, which represent 18% of the score; (3) project management details, which represent 30% of the score; and (4) budget and jurisdictional/disciplinary coordination issues, which represent 12% of the score.

The program funds can be used to support purchasing and deploying interoperable communications equipment; providing neighboring jurisdictions with the equipment or services they need to participate on existing networks; and the purchase or deployment of any other technologies that can be demonstrated to significantly increase interoperability within the public safety community of a given MSA.

Ideally, these MSAs are going to become models for successfully developing and implementing interoperable networks, and we want to be certain that they have any guidance that they may need during the development and implementation process.

Therefore, we have offered a variety of training and technical assistance resources to the grant recipients, working in consultation with the Department of Homeland Security. We have hosted a technical assistance kickoff conference that assists grantees with everything from handling the administrative requirements of the grant to addressing interjurisdictional liability issues related to interoperable networks. Our two agencies have hosted advanced technical assistance workshops, a National Interoperability Summit, and we have offered consultative services. Whatever form of technical assistance best meets the needs of a grantee—conferences, workshops, direct on-site consultation, or publications—we have sought to provide it.

Let me share some examples from the program with you. In Washington State, the City of Seattle and other cities within the Seattle MSA are working to establish a wireless data exchange system that will link their police and fire dispatch systems. The project also calls for their collective systems to be linked to the King

County Sheriff's Department, the jail system, Prosecutor's Office, Municipal courts, the State Police, and the state's Criminal Justice Information system. While there is still much work that must be done to get all of the existing systems to the stage that they are capable of linking, this system will allow officials throughout the Seattle MSA to share vital information and work together toward common public safety goals.

In Texas, the City of Austin, which is in Travis County, will use COPS funds to expand their existing 800 MHz regional radio system into neighboring Williamson County, and to upgrade Williamson County's older analog system so that it is compatible with Austin's. Once this project is completed, it can be used as a statewide benchmark that will enable state, local, and federal agencies to communicate on a common platform.

And, in Orange County Florida, COPS funds are being used to provide five shared communications channels across a nine-county region. First responders in nine counties will all be able to share and react to information in real-time.

This year, COPS was appropriated $10 million to continue the Interoperability Communications Technology Grant Program. Coordinating with the Department of Homeland Security, we plan to use these funds to make several grants and to support training and technical assistance that will assist the field and their ongoing efforts to improve interoperability. As in previous Budgets, the President's 2007 Budget proposes to focus support for first responder interoperability within Department of Homeland Security, which has a broader range of grant and technical assistance resources.

The potential of interoperable communications systems is tremendous and the need great. Thanks, in part, to these grants, police and fire communications and information systems will be developed in the future with an eye toward interoperability.

America has learned that tragedies, natural disasters, and crimes do not recognize jurisdictional borders. My neighbor's problem is my problem. When we act together, we are stronger than when we attempt to go it alone. First responders have accepted the challenge of achieving interoperability, and COPS is pleased to have been a partner with many federal agencies in a coordinated federal response to address this need.

Thank you, and I am happy to answer any questions you may have.

Mr. REICHERT. Thank you, and I do have a few questions. I will start out with general questions for the panel, anyone on the panel that wishes to respond.

With all the Federal agencies involved in this process in touching some piece or part of it, I am interested in who is keeping score, and accurate and timely and comprehensive Federal scorecard, if you must. Someone who is kind of tracking what we have done, what we are doing right now for interoperability, what we are going to be doing, what we are spending our money on, and what we have spent our money on, what has worked, what as not worked, just to ensure that the investments are actually matching the Federal plan.

If there is a Federal plan and I have heard some discussion about a Federal plan, but is there a watchdog? Is there one person responsible kind of overseeing this effort by the many Federal agencies.

Mr. BOYD. Ultimately, OMB, of course, is the watchdog, but what OMB asks us to do at SAFECOM is to look at all the departments' budgets that touch on wireless communications, that includes the independent agencies. Each year, OMB includes a requirement that before they can—before that money can be released, they need what amounts to a certification from SAFECOM that they are aligned with the national strategy. So we do that. We began that last year for the first time. We have done it again this year, and I assume we will do it again next year.

Honorable Henke. Sir, if I may, in addition to that, there are numerous things that are being undertaken. As Dr. Boyd mentioned

in his opening statement, there is the baseline review that will be coming out later this year. In addition to that, at the Office of Grants and Training, we have what we call our Biannual Strategy Implementation Report that I know we have provided information to your offices on before. That is how we track the expenditure of resources, and we can draw it down to counties and localities on what they are investing those resources on.

In addition to that, one of the things that we are undertaking and we are undertaking in partnership with and in cooperation with SAFECOM and other entities is our tactical interoperable communication plans, which are due May 1st. We are going to do full scale exercises on those. That will allow us, from a tactical interoperable communications standpoint, to see later in the fall where we are in those jurisdictions. We will be able to have those drive those investments for fiscal year 2007, and also identify lessons learned and how we take what we learn and then expand it to other jurisdictions, including the States.

Mr. REICHERT. Anyone else? So last year, Dr. Boyd, was the first time there was this kind of oversight to make sure the money spent was in line?

Mr. BOYD. Yes, sir. Last year was the first time that we had gone through that. Now, it is also important to understand a lot of other coordination activities that go on at the same time. In 2007, there will be a mandatory requirement that there be a State plan before grant funding can be provided to each of these activities. That is included, the Secretary has required that that be included in the guidance. The SAFECOM common grant guidance, which outlines how investments are made, again at OMB direction, has to be included in every grant program. It is included in the grants and training grant guidance.

It is included in the COPS office grant guidance and will be included as well in the allocations that come from the sale of auctions in the commerce department, and those discussions are already underway. So those will include the same kind of grant guidance.

Finally, we have an interagency coordinating commission activity, where we try to bring together all the Federal players, including the Defense Department, the Guard Bureau, all of the activities in DHS, in fact, all together in some eight different departments, to try to look at what everybody is doing, not all through grants. There are, for example, in justice programs that touch on interoperability because of the Department of Justice 25 cities project.

In the Customs Border patrol arena, there are a series of border pilots that are underway that also involve communications applications. We try very hard, to coordinate all of those at the same time, and to make sure they all comply with the national guidance.

Mr. REICHERT. What have we not done in this endeavor that we need to do immediately? What is the one thing that from this panel that strikes you as something we need to do now, that we need to commit to doing?

Mr. BOYD. Actually I think, let me be real clear. There is a natural tendency to wonder what is it the Federal Government can do to make this happen quickly? I would argue that the most fundamental requirement is that communities themselves commit to being willing to participate in developing interoperability. Now the

long haul part is our job. We have to be able to help to develop the standards. We have to provide the guidance, but at the end of the day, the individual communities are the ones who have to decide they are really going to make that happen. And every jurisdiction that has gone to work to develop the kind of agreements across jurisdictions and across disciplines that are required to do it, they have been able to achieve what we call emergency command level interoperability.

It is not the perfect interoperability we would like to have once we have a real standards regime in place and all the other things have happened, but it is something that can address the emergencies now. The public safety community has been very, very responsive to that.

So I think you are seeing a lot more multi jurisdictional efforts in a lot more places than has ever been the case before. So one of the things I think the national baseline is going to demonstrate is that there is a lot more happening in the field than is always apparent.

Mr. REICHERT. Mr. Pascrell.

Mr. PASCRELL. Mr. Chairman, in the next panel, Mr. Morgan is going to testify that to date, there is no quantitative or qualitative assessment of the nation's level of interoperability. Do you all agree with that?

Mr. BOYD. I think that is exactly true now. That is what the national baseline is designed to answer.

Mr. PASCRELL. When we say now, this is 5 years after 9/11 almost.

Mr. BOYD. When we took over SAFECOM in 2003, the very first thing we did was to impose a requirement to establish a baseline because we thought we needed to be able to figure out where we were measuring from. And so that is now underway to create exactly the kind of analysis you are talking about.

Mr. PASCRELL. Director Peed, I read your statement very carefully. The high in the COPS interoperability budget was a few years ago, $92 million. This year it is $10 million. And you spend a lot of time talking about COPS in your presentation, as you well know. I am not telling you something you do not know. And we are talking about how local communities must commit to the systems, Dr. Boyd, in order to have a system of emergency command level.

How do we expect local communities to commit to the system that we are trying to develop, and yet we have not developed the standards? How do you expect local communities to commit to the system without the resources.

Mr. PEED. Congress appropriated the funds obviously, and in their appropriations—

Mr. PASCRELL. I am sorry, Mr. Peed.

Mr. PEED. When Congress appropriated the funds for our agency, they included in our language the first year that we address the critical needs of law enforcement, and the second year funding required that we address the immediate needs of law enforcement. So we went out and partnered with all of our Federal partners to develop the program. We required the grants to be regional and multi-disciplined and multi-regional in effort, and then they were up to, in the first year, were up to $6 million per grant. And we

think there are some successes there in terms of meeting the immediate needs.

Mr. PASCRELL. Mr. Peed, every year you have a lower amount of awardees. You have less money. You have just started to touch the surface, and yet you are reducing the budget. In fact, you are trying to eliminate the budget according to your own numbers. I mean, how can you sit there and talk to us about the COPS program when the administration has tried to eliminate it? How do you do that? Tell me how you do that.

Mr. PEED. Since we had our funding in 2003, we have coordinated with originally the Office of National Preparedness, so we knew where our grants were going and that responsibility has now shifted to the Department of Homeland Security.

Mr. PASCRELL. Do you support the COPS program in your position with the Department of Justice?

Mr. PEED. Yes, sir.

Mr. PASCRELL. Do you think it should be fully funded.

Mr. PEED. It is funded, I think, given the priorities at the level I think the administration—

Mr. PASCRELL. What other priorities exist besides public safety, tell me?

Mr. PEED. Many of those priorities have shifted to the Department of Homeland Security.

Mr. PASCRELL. You mean to tell me now that the COPS program that the administration has tried to eliminate three times, you are telling me that that function, that activity is going to be adopted by some other Federal agency so we can look forward to the COPS program doing what it did in the 1990s to reduce crime in this country, to help reduce crime, you mean to tell me we are on track to do the same thing? We are going to be able to hire the same amount of police officers, is that what you are telling me?

Mr. PEED. The original goal of the COPS office was to add over 100,000 officers to the street. We have added about 118,000, so the Attorney General has testified before Congress on several occasions, both Attorney General Ashcroft and Attorney General Gonzalez that we have achieved that goal.

Mr. PASCRELL. We have achieved the goal. Okay. I want to come back to this later, Mr. Chairman. I find that incredible. Mr. Moran, back in 1996, the public safety community identified a need for 100 megahertz spectrum to accomplish their mission to communicate. Public safety will finally gain 24 megahertz. You brought that out in your testimony I think, in February of 2009. Is it not about time that the FCC does what it needs to do to allocate the necessary spectrum that public safety needs in your wisdom.

Mr. MORAN. Well, you are right, the 97 Budget Act, actually the 97 Budget Act directed the Commission to allocate 24 megahertz for public safety use, and it would not be available, as you know, until some time in the future when the digital TV transition occurred. In some parts of the country, that spectrum is available for public safety. In many parts of the country, it will not be available until 2009, as you point out.

Mr. PASCRELL. I come here as a friend, Mr. Moran, believe it or not. What is stopping us from implementing the urgent talk that

we all have on all sides of the table here? What is the main factor that stands in our way in your estimation?

Mr. MORAN. For, I think you are now referring to adequacy of spectrum, not interoperability.

Mr. PASCRELL. Correct.

Mr. MORAN. On the spectrum issue, the Commission, of course, is responsible for administering nonfederal spectrum. Frankly, the spectrum is being used by many parties. It is pretty much congested. The Commission has made a major effort, as a matter of fact, a coalition of public safety, Nextel and other 800 megahertz licensees came in to us and asked us to do some things to eliminate interference problems in the 800 megahertz public safety area. I believe the chairman talked about some of these interference problems last time that I testified.

The Commission, at the behest of this coalition, including public safety, we aggressively got into this, found a solution to not only eliminating the 800 megahertz interference spectrum that there therefore could make the public safety spectrum to be used more efficiently and effectively, but we also, through this process, there will be another 800 megahertz that will be freed up from that. So we are working on that. This was not a simple task. There were thousands of licensees in the 800 megahertz band that we are in the process of clearing out, to free this up for public safety, to give them a bigger band that is adjacent so their systems would work better.

Mr. PASCRELL. It would seem to me, I don't mean to interrupt you and there are other questions, and we would have another round, I assume. It would seem to me, Mr. Moran, and I thank you for your honesty. You have been very direct. I hope folks listen to what you just said. But I conclude, tell me I am wrong, tell me I am not perceiving what you said correctly, I am perceiving this as, well, public safety public safety will have to wait until the other interests decide to give up some of their space. Is that rather a cynical interpretation.

Mr. MORAN. Well, the 24 megahertz, in most places, will not be available until February of 2009. That is true. We are doing what the Congress has asked us to do there and that is the situation.

Mr. PASCRELL. But our frustration is, and I realize you can deal only as director in the department, but our frustration is to us there is nothing more important than the lives of our first responders. And to hear you and I know you are not, you are a very compassionate individual, I know a little bit about your background, do you wonder why we get a bit frustrated and a bit anxious and concerned? You do not have to answer the question.

This is unacceptable. We are going to wait for the private sector to give room to police and fire. We are not going to do that when you are forcing us to make regulations that we should not have to make. Do you understand what I am saying, Mr. Moran?

Mr. MORAN. I understand what you are saying, yes.

Mr. PASCRELL. Thank you. Thank you, Mr. Chairman for your patience.

Mr. REICHERT. Ms. Harman.

Ms. HARMAN. Thank you, Mr. Chairman. Thank you to you and the ranking member for holding four very interesting hearings on

this issue. I think as we assess the gaps in homeland security this issue of interoperable communications is the number one gap. I do agree that we have made some progress, but I don't feel that we are close to where we need to be, and part of that is Congress's fault. It would be nice to point fingers at these witnesses, several of whom I have worked with in other lifetimes, especially Dr. Boyd when he was at the National Institute of Justice, but it is not only their fault. It is our fault. Our fault, meaning Congress.

We made a promise to our first responder community and to the American people a decade ago that we would turn over dedicated spectrum for emergency communications by the end of this calendar year and we, we, the Congress of the United States, broke our promise. Several of us on this committee have been pushing for 4 years to enact H.R. 1646, the HERO Act, which would keep Congress's promise. HERO is still alive but it is not well. And instead, as Mr. Pascrell was just saying, Congress has punted and we will finally turn over spectrum in 2–1/2 years from now.

I am the ranking member on the House Intelligence Committee, and I receive scary briefings all the time. And I doubt that the terrorists who are plotting to attack us are waiting for 2–1/2 years until we can have an adequate framework for interoperable communications.

So my question to you is not to blame you for Congress's mistakes, but to see whether on an interim or patchwork basis we really are developing systems out there in our communities that can do most of this job. I hope the answer is yes. I am not sure that it is. But I just want to talk about for a minute some of the things that are happening in Los Angeles county and in some of the cities that I represent. Small cities are pooling resources. Los Angeles city and county which is a huge metropolitan area, is plugging into an I.T. base system with the capability to connect divergent frequencies. There is talk about creating a single platform of gateways, and also talk of building out a system of repeater networks so that this ability of ACU–1000 to integrate spectrum can be expanded and extended.

My question for the panel is are these strategies sufficient bridges to get us to 2009, or are we seriously, in my view, and you can respond, are we seriously inadequately fielding the interoperable strategies necessary to protect Americans in the event of terrorist or natural disasters?

Mr. BOYD. Well, I would have to say that the work being done in Los Angeles is probably some of the best effort in the country to try to bring together near-term interoperability. That is to achieve interoperable now with what you have. One of challenges, and nobody is comfortable with this, but it is the reality, is you have to start with what we have. There is a huge infrastructure there that cannot be changed that quickly. It is typically bought with the bond issue that takes anywhere from 20 to 30 years to pay off. So it is a very, very complicated thing to try to move it. In the meantime, Los Angeles has done a really, really solid job, in my judgement, of doing that. In the northern Virginia, southern New York area, for example, I was pleased when a few weeks ago, I was really pleased to hear from your committee staff that when they had gone out to talk to the communications officers and looked at

the communications centers in each of those places, they saw the continuum which we talked to you about before in the front of the tool box posted in every one of those communication centers with pins showing where they were on that process.

I would like to remind you what that continuum showed, because I think it is crucial, and that is that technology is only one of the critical lanes. There has to willingness and an agreement among the multiple jurisdictions and a number of Members of Congress here have helped to do that. You, Ms. Harman, did a lot of that in the early days when we first did a field hearing some years ago out in El Segundo, in helping to bring the communities together and get them to talk to each other and agree. Because once they are willing to make those agreements, we are not at a point that it is the cleanest kind of solution we want, but they can achieve emergency level interoperability now if they are willing to do that.

Ms. HARMAN. Does anyone else wish to answer the question. I know my time has expired, Mr. Chairman. I would just like to have the answers for the record.

Mr. MORAN. Yes, may I. Yes, I think some of the things you are mentioned, I.T.-based technologies to interconnect existing public safety systems that are operating at different frequencies and different modulation techniques and all of this, I think that there are real potentials here to have some real improvements in interoperability that can be achieved in the short term.

When the 24 megahertz is fully available in a couple of years, that is the first step. Systems have to be built. A lot of money will have to be spent to put these things in. And with the new systems, the FCC, by the way, has rules that the new 700 megahertz systems, we have set aside some interoperability channels and we have made a requirement that all 700s, that all the radios associated with them have to be able to access these interoperability channels. But there is still going to be the question, how about all the embedded base? Will those things be able to interoperate with the 700?

We think there are a number of technologies out there that will help us make some substantial progress in interoperability in the short term. It appears that the amount of capital needed to do it is much less than full scale change out of these systems. But I certainly agree with Dr. Boyd that it is not just the technology. You have to have the local authorities to agree that this is what they want to do. You have to have them work out how these systems are going to work, who is going to be in charge, how it will work tactically and strategically, and you have to train all the people to make this thing work. It is a lot more than just buying the technology. There is a lot of human element here and it is all essential. But nonetheless, I think progress can be made in the short term with solutions like this.

Mr. REICHERT. The gentleman's time has expired. Mrs. Christensen.

Mrs. CHRISTENSEN. Thank you, Mr. Chairman. Probably part of this have already been answered, but the last, or the most recent example of interoperable communications not working was Katrina, and have you responded already as to what your assessment has been of what went wrong in Katrina and given the fact that we are

just a month and a half from hurricane season and a disaster could happen at any time, based on what went wrong then, what has been done to ensure that by June 1st, that some of these problems will not recur?

Mr. BOYD. I think the first thing to understand is that the principal problem in Katrina was the failure of operability rather than interoperability. The whole basic system went out.

Mrs. CHRISTENSEN. But that could happen in any—if I was a terrorist, I would take that out first.

Mr. BOYD. That is correct, but if you do not have that communications infrastructure in place, you cannot even get to interoperability. In Katrina, you had a combination of things. You also lost a power grid. By losing the power grid you lost your ability to even charge batteries and handheld units. So that is why it took some days to put it back together. You lost the powers. You lost the power grid. You lost the ability to charge those things over an area about the size of the United Kingdom, now that takes some time to recover.

Mrs. CHRISTENSEN. I live in the Virgin Islands. We have had hurricanes, power outages. It would seem to me that we should have learned how to deal with those issues already. No one—does anyone else have an answer?

Ms. HENKE. If I can tell you some of the things we are undertaking, some of the things we are working on to address those issues. One, as I mentioned prior to your arrival, is tactical interoperable communications, the plans that are due on May 1, and the exercises that will occur that will identify shortfalls and gaps.

In addition to that, before hurricane season starts, the Department of Homeland Security in coordination with multiple agencies within the Department as well as outside the Department, with our State and local partners, is conducting hurricane exercises along the eastern seaboard and the Gulf Coast. Those exercises will look at evacuation as well as communications and help us to once again test some of the things that have been corrected or fixed since Hurricane Katrina and also identify where some of those gaps are and how we can potentially quickly address those.

Mrs. CHRISTENSEN. Thanks for the answers. I am still not very comfortable and I am just always amazed at what we have not learned over the years of having gone through hurricanes.

The integrated wireless network, I am not sure who I should direct this one to, but it is to provide a consolidated nationwide federal wireless communication service and the partnership started in October, 2001. We are now four and a half years into this. How many of the 80,000 law enforcement users or 2,500 sites have been served? That is SAFECOM. Department of Defense I guess it would be.

Mr. BOYD. There are two elements to that. DHS has a role in it and the Department of Justice are partners. That is not the program in my office. I can't tell you how many sites have been in place. What I can tell you is that there is an extensive collaboration involving SAFECOM, the Department of Justice, the Office of Grants and Training, and the National Guard Bureau and others, in trying to make sure that as that interoperability is established in those major cities, that it also fits within the larger national con-

struct, but I can't give you the details on the program because the manager for that is in the Wireless Management Office in the Department of Justice.

Mrs. CHRISTENSEN. Thank you. Another question to the Department of Commerce. Mr. Moran.

Mr. MORAN. I believe the NTIA person is not here.

Mrs. CHRISTENSEN. Okay. I guess I came in late. I will let that be my last question on this round.

Mr. REICHERT. Mrs. Lowey.

Mrs. LOWEY. Thank you very much. I want to thank the chairman and the ranking member for holding this hearing again, although we have been looking for answers for a very long time. Some of us have been working on this for 4 years. Before I get to the immediate question, just following up, I believe Dr. Boyd said the problem in Louisiana was communication, not interoperability.

Now I am not an expert in this area, although many of us have been working on this for 4 years, but I believe Director Moran is Director of the Office of Homeland Security Federal Communications Commission. Now it would seem to me that yes, the communications got flooded; yes, it all broke down. This is the United States of America. What does the military do in situations like this? Can't you preposition equipment that can be used?

Four experts here. We are just trying to look for answers with great respect for your expertise. Shouldn't you be able to say to me, Dr. Boyd, Mr. Moran? Don't worry about it, we know how to preposition equipment, whether it is on trucks or on a high ground or whether using equipment that you plug into. How can you sit there and say we didn't have interoperability but now I can't guarantee you they will be able to communicate because that is a communications issue, not an interoperability issue.

And then you were saying, I believe it was Dr. Boyd, I am not sure, might have been Mr. Moran, again, I apologize, that this gets more complicated as we move along because many communities who aren't going to wait for you guys, they are fed up with the Federal Government, are taking out bond issues to buy communication. And in many instances, because there are no Federal guidelines, which we were told by Secretary Ridge 2 years ago they were going to be in place. Okay. They are moving ahead, and as you said, it gets more complicated.

Now I understand this is extremely complex, it is a time consuming issue, but, again, we have known about all of this for years, and 9/11, where we lost hundreds of lives, many could be attributed to the fact that they couldn't communicate.

The final report of the Federal Public Safety Wireless Advisory Committee concluded, quote, unless immediate measures are taken to promote interoperability, public safety agencies will not be able to adequately discharge their obligation to protect life and property in a safe, efficient and cost efficient manner. That report was written over 9 years ago. Not 4 years ago, 9 years ago.

Okay. You are all in charge here. We are just trying to move this along and to understand why you can't get it done. So looking at the broader picture, when will we reach a point where we understand this is an emergency. We could have a real problem with the storms in about a month and a half, or month. When will our com-

munications system not be a liability? What steps have been taken specifically to bolster communication systems in hurricane-prone areas since the Katrina debacle? Because you are going to tell me, and I heard this well, we are studying it, in 6 months, in a year. No wonder the public says what is this whole apparatus. You have hundreds and hundreds, thousands of people working on this and yet our citizens are not safe because you haven't come up with even a temporary answer.

You can come up with a better answer a year from now, 2 years from now, but what have we done, how can you tell us and the people down there or another hurricane area that this is going to work, they are going to be able to communicate, that it won't be the days of Paul Revere where someone from a roof had to throw down a glass jar with a message in it? Can you give us any confidence that you are doing something that is worthwhile, that is going to keep people safer, that is moving along and making us able to— don't know if I even want to stick to interoperability— being able to communicate in an emergency. If I sound frustrated, I apologize, but I am.

Mr. BOYD. First, I didn't use the term "communicate," I said "operability." That means you have a communication system able to provide communications among all of the elements of that agency. Interoperability refers to the ability of that agency to communicate with another agency.

Mrs. LOWEY. Talk about the first because you have told me the problem was everything went down. What have you done, what technology is out there, what does the military have to address operability?

Mr. BOYD. As a soldier retired after 23 years of combat service the first thing the military does is take anywhere from 5 to 15 days to put in a new infrastructure to bring in the things they need to cover that area. They don't do it overnight. I know there is a comic book notion that the military drops in and communication takes place. That does not happen.

Mrs. LOWEY. Can you preposition material?

Mr. BOYD. You can preposition materials but you are going to have to preposition them outside the affected area because you don't want them destroyed by the storm, which means you always stock with the painful reality that you have to move them. That takes time. Not only do you have to move them, you have to figure out where you are going to put them when you get there.

So some of the best sites were under water. The towers were gone. You can't replace a 300-foot tower with a hundred foot tower that you can stick into an airplane and move into place. So you are always going to have to do the best you can in that kind of environment.

What I think is most important, and I was involved in the PSWAC study back then, is that more for interoperability has occurred in the last probably 4 or 5 years than I saw in the entire time I have been involved in interoperability. But the point I want to make and have been trying to make repeatedly in every hearing is whether we like it or not this is going to take some time. This is a huge, huge expensive infrastructure that greatly exceeds a hundred billion dollars just for the infrastructure itself. Of that,

most of it is legacy equipment, so whatever standards we build now has to figure out how to connect to some of these old systems.

I had a county commission ask me to come down last week and help them figure out how to go about moving to a 700 megahertz system because they are currently on 4.9 gigahertz. They built that—or a 490 megahertz system. They built that in 1985. It is 21 years later. If they could get the county commission now to approve, using a combination of straight grant money and their money, a new system, it will take, and this is the normal for any communication system, 5 to 10 years, if the money is available, the licensing is available, there aren't any problems with environmental impact statements, they can get the towers built, no not in my backyard problems; it takes 5 to 10 years under perfect circumstances to build a new communications system.

So none of this will happen overnight. But I will tell you that a great deal has happened. What is most refreshing is what is happening in the regions themselves that are beginning to address this work. The Mississippi Wireless Commission asked me to come down so they could talk to me about what they were doing. Last month Montana came down to see me, or last week, and Montana pointed out that they have built a new plan, everybody on board in the State, so that they have been able to reduce the number of towers, the most expensive piece of a communications infrastructure, from 33 to cover their northern border, which is one time zone wide, to 11. One-third the cost because they got everybody together. But the important issue is they got everybody together. Although we at the Federal Government like to think we are driving the whole train, the reality is it is that local level and those States that will drive that train. We can help by offering the tools, we can help by offering them the guidance.

The public safety community will tell you that they like the SAFECOM guidance because that is exactly how they think they need to build those communications systems. And we can help with grant money to focus things in the direction we need to have things go. But we will not at the Federal level force a dramatic change in 1 or 2 or 3 years. The communities will make that happen, but it will take them within the period of time it takes them to replace an existing infrastructure that has a lifespan of 15 to 30 years.

Mr. REICHERT. The gentlelady's time has expired.

Mr. Peed.

Mr. PEED. I wanted to follow up. As Dr. Boyd said, this was a 90,000 square mile area, an area the size of Great Britain. I just got back from there, I spent 6 days and I toured through Biloxi and New Orleans and the parishes talking to sheriffs and chiefs and it was interesting that some little organizations like Slidell did not lose communications even though they lost half their tower.

New Orleans in its entirety lost all its communications, including the FBI. They couldn't even make cell phone calls. What the COPS office has done is we have made a number of grants to those gulf regions. We have made grants to Birmingham, Shreveport, Baton Rouge, New Orleans and Mobile, just to name a few. And New Orleans had partnered with five of the parishes there to develop an interoperable communications system to protect their ports as well as respond to emergencies of this measure.

Mrs. LOWEY. I know I would be out of order but I know we would all like to hear, could the gentlemen just follow up, why did Slidell not lose power?

Mr. PEED. I don't know exactly why. It would require a technical person to take a look at that, but I sat with the chief there and he was showing me pictures of his cruisers under water and his towers located there has not been rebuilt yet but they still have radio communication. It would take a technical person to take a look at that.

Mrs. LOWEY. Mr. Chairman, I know this is out of order again, but just following up with the gentleman.

Mr. REICHERT. Do you have one additional question for the gentleman?

Mrs. LOWEY. I just don't understand it. I wonder how often you have briefed Secretary Chertoff. Could you tell us in writing at another time because my time ran out already the state of communications in ever locality in the country? And if something like that is successful in Louisiana, I would think coming before this committee we would be briefed or you would be immediately following up on what was successful and recommending that.

I would appreciate it, Mr. Chairman, if we don't have it, if we can get a briefing that I am assuming you give to Secretary Chertoff at least once every other week, or something like that, with the state of communications across the country and are there other examples like that that could be

Mr. REICHERT. What we will do is we will have the staff coordinate with the panel of witnesses and see if we might be able to arrange that.

Mrs. LOWEY. Thank you so much.

Mr. REICHERT. You are welcome.

We will have a second round of questions. And I have a couple of questions. I would like to go back to the issue of reconfiguring 800 megahertz. I just want to make it very clear that this has been a lot longer than 4 years that we have been struggling with this issue. I know some Members of Congress have been involved in this process for that long.

But back in 1997 when I first became the sheriff of Kane County we were still on a VHF system and transitioning to 800 megahertz, and since 1997 as we transitioned to 800 megahertz, and maybe you are familiar, I know Carl has visited Seattle, and Dr. Boyd, familiar with the King County area and the inability of 800 megahertz to serve the needs there, especially the foothills of the Cascades and sometimes downtown within the inner city area with the tall buildings, especially with the firefighters and police officers together, their inability to communicate on 800 megahertz.

So we have been hearing about the reconfiguration of 800 megahertz for almost 10 years. That has been a frustrating thing for first responders to be patient because now we are told to be even more patient. And we are tired of waiting, I guess is the message that I want to deliver. I understand the complexities of the problem but it seems to me nothing can be more important than the safety of our first responders, and to put some business ahead of that doesn't seem to be—doesn't seem to be—is not the right thing.

I would like to ask Assistant Secretary Henke, NTIA has a $1 billion grant program for interoperability; do you think they should have that within their jurisdiction to manage and disseminate, or should that better be placed in your shop?

Ms. HENKE. I can tell you that Congress provided the money to NTIA. I can tell you NTIA and the leadership of NTIA as well as myself and members of my staff have met and have discussed those resources. The goal of both NTIA as well as the Office of Grants and Training at DHS is the most effective and efficient use of those dollars to have a measurable result on interoperability.

So whether it is housed and transferred to Grants and Training or whether it stays within NTIA, I can assure the Committee that we are already talking and coordinating to make certain that we have—that those resources accomplish a measurable result.

Mr. REICHERT. Wouldn't it make sense though to have that money in your shop rather than have another entity to communicate with, coordinate with and make sure that we are spending the money on the strategic plan that has been described?

Ms. HENKE. That is a possibility. Congress provided the resources to NTIA. We have had those communications and I can assure you that once again in the language it says that NTIA should coordinate with the Department of Homeland Security and with the SAFECOM guidance. Our goal once again is to make certain that it is the most efficient way for our first responders. And so if that means transferring it to the Office of Grants and Training in the end for us to administer those funds, if that is the most efficient way, we will do so.

Mr. REICHERT. There is discussions taking place, I know. Thank you.

Dr. Boyd, you mentioned an interoperability baseline survey. Did it include, the survey include questions around standards?

Mr. BOYD. Not so much—what we did was to build the baseline survey around the interoperability continuum. We didn't build it specifically around standards. And the reason we didn't is that there is no standard now that can cover the range of equipment used in the field and the survey does look at what are some of the kinds of different technologies you use.

We think standards are a forward-looking activity where we have to build in hooks and ability to get to those legacy systems, but it is not so much a backward-looking activity.

Mr. REICHERT. Wasn't this a voluntary survey?

Mr. BOYD. It is a voluntary survey. It will go out very shortly. It will go out to 23,000 different police, medical, fire service.

Mr. REICHERT. So it hasn't gone out yet? We have already spent $2.2 billion on interoperability and we are just now doing a survey?

Mr. BOYD. When SAFECOM came to DHS, one of the first things we decided we needed to do was a baseline survey. So when Congress appropriated funding in 2005 we immediately started the contract to get into place the survey and design that survey.

Mr. REICHERT. I will yield my time.

Mr. Pascrell.

Mr. PASCRELL. Thank you, Mr. Chairman.

Mr. Moran, the FCC's strategic plan recognizes that over 90Rrcent of the Nation's communications system is privately

owned. The Department of Homeland Security has stated that 85Rrcent of the Nation's critical infrastructure is owned by the private sector.

I have a couple of questions for you. What tools does the FCC have to mandate that the products marketed for interoperability live up to their claim? What tools do you have, what power do you have, what authority do you have? That is my first question.

Mr. MORAN. Well, what tools do we have that can assure that products manufactured to promote interoperability do in fact provide interoperability? To the extent it is a radio product, the product has to be certified by the FCC. So perhaps there is something there if it is a radio-based product. If it is an IP-based product, I don't think that is the issue there.

I don't know that the FCC requiring the products—that products meet the criteria that they are designed for, that is not a normal process that the FCC is involved with.

Mr. PASCRELL. Is that your answer? Do you wish to make a phone call?

Mr. MORAN. I better check back with the people back home.

Mr. PASCRELL. The second question—am only being serious. How does the strategic plan, Mr. Moran, fit within the Department's plans for proposed Public Safety and Homeland Security Bureau? How does that strategic plan fit into the Department's plans, Homeland Security department's plans?

Mr. MORAN. How does the FCC's plan to reorganize fit into the Department of homeland security's plans? I don't really know the answer to that but I will say this; the FCC, myself included, deal routinely with a number of segments of the Department of Homeland Security, most notably the national communications system. But other parts with FEMA and other parts, and we work closely with them on joint issues, including the national response plan in which the FCC is a support agency to ESF2 function, emergency support function number 2 communications, for communications response when a major disaster takes place. We work closely with them. We do that now.

When the commission reorganizes, which we believe it will here if this is all approved, we intend to work just as closely with the Department of Homeland Security on the same kinds of things after the reorganization. We hope we will be able to actually do a better job in that coordination because we believe by bringing all the focus of all the national security, homeland security, emergency things in one part at the FCC, we will have a more comprehensive, effective unity process there so that we can work better with Department of Homeland Security and Justice and others that we need to work with.

Mr. PASCRELL. Because, Mr. Moran, if the figures are right, and I think you would agree with them, 85 or 90Rrcent of the Nation's communications systems, it would appear to me that the enforcement power of FCC is going to have to be very definitive, and how far are you willing to go in terms of what was said previously. I am very concerned about this because you are an independent agency, and you should be. Or should you be? Do you have the power to enforce what you have talked about today, which I think is going to be another question.

Mr. Chairman, I have a lot of questions, I am going to submit them for the record, and I want to thank the panelists for their cooperation today.

Mr. REICHERT. Thank you, Mr. Pascrell. No further questions?

Mrs. LOWEY. I will save it until after we get that report. Thank you.

Mr. REICHERT. Thank you, Mrs. Lowey. I would like to thank the witnesses again for their valuable testimony. This panel is excused, with the exception of Dr. Boyd, whom I hope will also sit on the second panel for purposes of responding to our questions related to standards and technology.

The Chair now calls the second panel. Thank you all so much for being here.

Good afternoon. With us on the second panel today, Dr. Boyd, welcome again. Dr. John Morgan, Assistant Director for Science and Technology, U.S. Department of Defense; Mr. Dereck Orr, Program Manager, Public Safety Communications System, National Institute of Standard and Technology; Mr. Jim Gass, Deputy Director, National Memorial Institute for the Prevention of Terrorism; and Mr. Bruce Walker, Chairman, Subcommittee on Government Affairs Committee, Homeland Security and Defense Business Council.

Mr. REICHERT. The Chair now recognizes Dr. Morgan to testify.

STATEMENT OF JOHN MORGAN

Mr. MORGAN. Thank you very much. Good afternoon, Chairman Reichert, members of the subcommittee. I am pleased to appear before you today on behalf of the Department of Justice to speak to you on the issue of public safety communications. I will address the need for a complete set of standards and a compliance testing program, new technology development and the role of independent evaluation of interoperability programs.

NIJ, the National Institute of Justice, is a component of the Office of Justice Programs. Its mission is to advance scientific research, development and evaluation to enhance the administration of justice and public safety. Our primary focus is on State and local criminal justice agencies, which are responsible for over 95Rrcent of the investigation and adjudication of crime in the United States. NIJ is the only Federal agency dedicated to improving the effectiveness of criminal justice through scientific research.

NIJ has a great deal of experience with regard to assistance programs related to technology and other criminal justice needs. For example, Mr. Chairman, NIJ administers the President's DNA initiative, and I know you are very familiar with the power of DNA to solve violent crime.

NIJ has been involved in addressing public safety communications issues for over a decade. Through its communications technology portfolio, also know as CommTech, NIJ pursues short and long-term interoperability solutions involving wireless radio systems and information technology. CommTech, like all of NIJ's portfolios, relies on a Technology Working Group of frontline practitioners to identify the most critical technology problems that will receive investment from our agency. These law enforcement and

public safety practitioners have identified standards development and compliance assurances among their highest priorities.

Mr. Chairman, NIJ strongly recommends the adoption of a full suite of standards and a compliance testing program to ensure compliance of federally funded systems with those standards. To achieve this will require a very close coordination among all of the Federal entities here today and NIJ welcomes even closer coordination among our Federal partners.

NIJ suggests that any Federal assistance funding program targeted to public safety communications include independent evaluations of program outcomes. These evaluations should focus on compliance with standards, assessment of the fielded systems against the SAFECOM Statement of Requirements, the improvements in interoperability and operability that those systems produce. Such evaluations should also include fundamental examination of public safety benefits such as improvements in response to critical incidents.

Federal assistance programs in interoperability have thus far lacked such independent evaluation. Because of this there is no objective data on their impact, whether positive or negative.

NIJ also recommends that continuing technology research and development be a central part of the Federal Government's role in public safety communications. While a comprehensive suite of standard and effective policy coordination are essential to addressing the issues of public safety communications, new technology development is also critical for success in this area.

NIJ has focused its research and development investment on Cognitive Radio and Software-Defined Radio technologies because we believe these emerging tools may enable first responders to communicate seamlessly at critical incidents in the future. These and other technologies will improve interoperability and operability; that is, the ability to communicate reliably under normal circumstances.

Mr. Chair, spectrum allocation is a major problem for the effective deployment of interoperable and operable communications systems. One approach has been to increase the spectrum available to public safety agencies. Another approach, which NIJ is pursuing, is to develop technology that will enable public safety agencies to better use the spectrum allocated to them. Through current and future grants, focusing on cognitive radio technologies, frequency allocation coordination databases and other approaches, we believe greater access can be attained by public safety in the existing spectrum on a day-to-day basis and during emergency or disaster situations.

NIJ has devoted an average of $13 million per year to its CommTech portfolio. A remarkable amount of work has been done through this focused investment. In addition to technology assistance, standards development and testing, NIJ funds approximately 20 research and development and demonstration projects each year. Among our accomplishments, NIJ funded development of the Virginia Statewide Communications Interoperability Plan, a national model for State level planning and cooperation. With the support of the FCC, NIJ also funded the development of the Computer-Assisted Precoordination Resource and Database System

which is used to plan and use regional frequency spectrum more efficiently.

NIJ convened the National Task Force on Interoperability and published the *Why Can't We Talk* guidebook as well as a wide range of other technical documents for practitioners, such as our *Understanding Wireless Guide.*

Every day, through our center system, NIJ provides technology assistance around the country. In particular, the NIJ's Western Center has supported CommTech efforts in software, radio as well as responding to calls for technology assistance defined.

Mr. Chairman, a single entity or even the entire Federal Government will not solve the interoperability challenge alone. Clear delineation and better coordination among Federal entities is certainty beneficial. Although the challenges in public safety communications will take many years to solve, the Federal Government can play a very positive role through a comprehensive, coordinated and standards-based approach.

My full statement has been submitted in writing for the record.

[The statement of Mr. Morgan follows:]

PREPARED STATEMENT OF JOHN S. MORGAN

APRIL 25, 2006

Good afternoon Chairman Reichert, Mr. Pascrell, members of the Subcommittee. I am pleased to appear before you today on behalf of the Office of Justice Programs' National Institute of Justice (NIJ) to speak to you on the issue of public safety communications interoperability. I will address communications interoperability needs of state and local law enforcement and public safety, especially with respect to emerging technology and the need for standards.

Congress created NIJ in 1968 as the research, development and evaluation arm of the U.S. Department of Justice (DOJ). Its mission is to advance scientific research, development, and evaluation to enhance the administration of justice and public safety.

NIJ's primary focus is on state and local criminal justice agencies, which are responsible for over 95 percent of the adjudication of crime in the United States. NIJ is the only federal agency dedicated to improving the effectiveness of criminal justice through scientific research. NIJ is committed to the scientific process of open competition, peer-review, published reports and archived data. NIJ's Office of Science & Technology (OS&T) was established in 1992 to execute the agency's technology research and development program. This program includes: technology research and development; establishment and maintenance of performance standards for test and evaluation of technologies and equipment; and establishment and maintenance of the National Law Enforcement and Corrections Technology Center (NLECTC) system. The NLECTC system supports NIJ through development of technology requirements, test and evaluation, and providing technology assistance to state and local agencies through 10 technology assistance and specialty centers across the United States.

Although OS&T has been in operation for more than a decade, Congress officially recognized the office in Title II of the Homeland Security Act of 2002 (HSA). Through that legislation, Congress assigned several critical responsibilities to NIJ, including:

- To establish and maintain advisory groups to assess the technology needs of federal, state and local criminal justice agencies;
- To establish and maintain performance standards, test and evaluate law enforcement technology and equipment, and establish programs to certify, validate and mark technologies and equipment conforming to these standards;
- To take the lead in establishing a coordinated federal approach to issues relating to criminal justice technology; and
- To administer a program of research, development, testing, and demonstration to improve the interoperability of voice and data public safety communications.

NIJ has extensive experience in addressing public safety communications issues. Through its Communications Technology portfolio (CommTech), NIJ pursues both short- and long-term interoperability solutions involving wireless telecommunications and information technology. NIJ's work in this area includes:

- Research and development of technology for wireless interoperability;
- Test and evaluation of current products;
- Standards development for wireless interoperability;
- Pilot demonstrations on cutting edge technology; and
- Technology assistance to state and local agencies.

The CommTech research and development efforts are concentrated on Software Defined Radio (SDR), cognitive radio, Voice-over-Internet Protocol (VOIP), Advanced Wireless Voice and Data, and in-building location and communication technologies. As in all of its technology portfolios, NIJ maintains a practitioner-based Technology Working Group (TWG) for the CommTech portfolio comprised of state and local practitioners who offer advice on technology requirements and program direction. NIJ's CommTech investments are based on the specific needs identified to us by this TWG. NIJ also coordinates its program with all the federal agencies involved in public safety communications interoperability, including SAFECOM and the Office of Grants and Training in the Department of Homeland Security, the National Institute of Standards and Technology within the Department of Commerce, and the Office of Community-Oriented Policing Services within the Department of Justice.

These front line practitioners have identified standards development and compliance assurance as among the priorities in this area. Only a very small number of standards exist to ensure that radio systems are interoperable across jurisdictional and agency boundaries. In addition, there is no compliance testing program to ensure that systems conform to the few standards that do exist. Compliance testing is an integral component of any standards development effort to ensure that fielded systems meet the requirements of standards.

While federal assistance programs for interoperability already include technical assistance for state and local agencies, more independent evaluations of the outcomes would be advisable. Evaluations should focus on actual compliance with standards, assessment of the fielded systems against the SAFECOM *Statement of Requirements (SoR) for Public Safety Wireless Communications and Interoperability,* and the improvements in operability and interoperability those systems produce. Such evaluations would also include fundamental examination of public safety benefits, such as improvements in response to critical incidents. Federal assistance programs in interoperability thus far have lacked such independent evaluation, therefore there is insufficient data on the impact, whether positive or negative. NIJ has a close working relationship with SAFECOM and has played a primary role in the initial development of the SoR and in its ongoing review.

The Role of Technology Development

Developing a comprehensive suite of standards and effective policy coordination are critical to addressing the issues of public safety communications interoperability and operability; but developing new technology is also vital. NIJ believes the issues of operability and interoperability are inextricably linked. Operability means that two individuals from the same agency can talk with each other. Operability deals with issues such as equipment availability, bandwidth and spectrum allocation issues for voice and data, interoperability between vendors and technology, standards, command and control, and federal, state, and local coordination. Interoperability occurs when two (or more) individuals from different public safety agencies communicate with each other. Without operability, interoperability is irrelevant. Focusing solely on interoperability will not allow the practitioner to communicate or access information effectively.

Although technology development alone will not solve all communications problems, it can provide important solutions that enable public safety to access the revolution in wireless communications underway in the commercial market. For this reason, NIJ has made significant investments in new technologies such as SDR, cognitive radio, and satellite communications for rural agencies. Such technologies should enable public safety practitioners to "roam" freely just as cell phone users do and maximize the potential of the limited radio frequency spectrum made available to the public safety community. Of course, this can take place only when standards are in place to ensure that systems will be compatible with each other through advanced technology. Any federal investment in communications should recognize the need to develop technology solutions that enable improved operability and interoperability. Cognitive radio and SDR may enable first responders to communicate seamlessly at critical incidents in the future.

A SDR radio is one where frequency range, modulation or maximum output power can be altered by making a change in software without making any changes to hardware components that affect the radio frequency emissions. SDR may provide an efficient and comparatively inexpensive solution to the problem of building multi-mode, multi-band, multi-functional wireless devices that can be easily enhanced. As such, SDR can be considered an enabling technology that is applicable across a wide range of areas within the wireless industry, not just public safety.

Through CommTech, NIJ is funding the Public Safety Special Interest Group (PS SIG) within the SDR Forum. The goals of the PS SIG are to raise awareness of SDR, to publicize the activities of the Forum in addressing issues confronting public safety, and to increase participation of the public safety community in the SDR Forum. One of the Forum's more important undertakings is a study to assess the potential of, and issues associated with, SDR technology for the public safety community, with emphasis on disaster response. The report was approved by the SDR Forum membership this month (April 2006).

One specific SDR development example is the Dynamic Open Architecture Radio System (DOARS). DOARS is a collaboration with the U.S. Navy's Space and Naval Warfare System Center-Charleston. The project heavily leverages work in SDR projects within the Department of Defense, and seeks to create an affordable, user-friendly PC-based "universal radio" for public safety agencies.

A cognitive radio is a step beyond SDR. Whereas an SDR requires human programming, a cognitive radio will have the ability to adapt its behavior based on external factors without human intervention. A cognitive radio can alter its transmitter parameters based on interaction with the environment in which it operates, i.e., it senses what systems a radio can connect to and connects to them. This interaction may involve active negotiation or communications by the device with other devices or passive sensing and decision-making within the radios. A cognitive radio may be able to change its operating frequency to optimize use, sense signals from other nearby transmitters in an effort to choose an optimum operating environment, modify transmission characteristics, waveforms, and transmitter power to allow greater sharing of spectrum, select operating parameters based on what power and frequency are allowed at its current location, and implement "device-negotiated" sharing of spectrum under the terms of a prearranged agreement between a licensee and a third party. Cognitive radios may eventually enable parties to negotiate for spectrum use on a real-time basis, without the need for prior agreements between all parties. Of course, this will be important to both commercial and public safety customers who have limited amounts of radio spectrum available.

NIJ is funding Virginia Polytechnic Institute and State University to build a prototype cognitive radio that can recognize and interoperate with commonly used public safety waveform standards. This work leverages National Science Foundation investments to develop and test cognitive radio techniques for commercial applications.

Spectrum Allocation

Spectrum allocation is a major requirement for the effective deployment of interoperable and operable communications systems. One approach to dealing with this difficulty has been to increase the spectrum available to public safety agencies. Recent legislation that sets a date certain for the digital television transition will facilitate the reclamation of valuable spectrum resources for public safety use. This spectrum is anticipated to enable greater interoperability among public safety agencies. Another approach, which is being pursued by NIJ, is to develop technology that will enable public safety agencies to better use the limited spectrum allocated to them. NIJ is funding multiple efforts to develop such technologies that would be of use to state and local agencies receiving Federal grant funds.

In the current fiscal year 2006 solicitation cycle, NIJ is looking to fund technologies that will utilize the newly allocated public safety bands more efficiently. This includes technologies that involve mesh, or ad-hoc, networking that operate in the 4.9 GHz band and, in the future, the 700 MHz band. We believe these efforts will allow more effective and productive use of existing bands and quicker identification of additional bands if needed to meet national objectives for our first responders.

The Current Status of Standards

It cannot be over emphasized that developing standards is vital to dealing with the issue of public safety interoperability. Long before September 11, 2001, NIJ recognized the importance of interoperability standards for the public safety community. NIJ, through CommTech, is deeply involved in development of the APCO (Association of Public-Safety Communications Officials—International, Inc.)—25, or Project-25 (P–25) standard. This initiative is an industry-wide effort to set voluntary

standards for digital two-way radio technology for public safety organizations. In the early 1990s, the P–25 Steering Committee approved the very first public safety, user-driven Statement of Requirements (SoR) with the support of NIJ's CommTech Program.

NIJ funds the chairmanship of the P–25 standard steering committee, a public standards committee under the Telecommunications Industry Association, and the travel costs of some of the public safety agency representatives who participate in the process, thus helping to ensure objectivity and representativeness in the standards process. While these costs are small, less than $250,000 per year, they have provided both the impetus and the core element of a truly user-driven standards process. Within P–25, the steering committee and its user groups determine the user requirements, the standards that are acceptable, and the priority of developing those standards. Through that funding, we have leveraged the extensive economic resource of the major public safety telecommunications industry in a cooperative and consolidated effort to improve competition, provide interoperability, and ensure a transparent and achievable migration path.

Since P–25's inception, the P–25 steering committee and its partners in the Telecommunications Industry Association (TIA) have completed over 34 technology standards that will provide one of the three primary legs in our long-term efforts to create public safety interoperability. Long-term planning and interagency cooperation will also be necessary to implement interoperable communications systems across the nation.

Although significant progress has been made, there are a number of standards that need to be developed. These include:

- Inter-Sub-System Interface (ISSI) which allows a mobile from one system to transparently roam into another compatible system and have complete communication.
- Enhancement to the Fixed Station Interface to ensure easier and more complete console access.
- Enhancement of the Consol Interface Standard to ensure greater transparency.
- Completion of the Network Management standard interface.
- Enhancement of data interface to ensure transparent system-to-system data transport on a more ubiquitous bases.
- Enhancement of mobility to improve upon ease of access during roaming.
- Telephone Interconnect—ISSI compatible

A multitude of other conformance and performance standards are also needed, including interface standards for such things as global position systems or other user requirements as they arise. A total of as many as 90 standards are anticipated. The new standards that are required will be much more abbreviated than the current 34 since they will be based on many of the original standards and modified to fit the need of the next technology platform. Of course, all these new technologies and associated standards must be compatible with existing systems and standards. Public safety agencies do not have the resources to replace entire systems every few years. Even beyond these standards, there is a complete suite of needed standards that relate to spectrum efficiency. Finally, there is work continuing on broad-band data and 4.9 GHz data standards to allow the transport of high-speed wireless data among field radios and to and from major Public Safety Answering Points or Incident Management Centers. In short, there is a great deal of work that needs to be done to address standards for public safety communications.

Testing and validation of P–25 compliant technology is necessary to ensure the equipment being sold is interoperable at all levels. While there is significant compliance at the level of common-air-interface, there have been problems with the interoperability of features and functions. The P–25 steering committee, its user groups, TIA and its members, with the support of NIJ, have been aggressively working with the Department of Commerce's National Institute of Standards and Technology's Office of Law Enforcement Standards, the Institute for Telecommunications Sciences, and SAFECOM, to develop a coordinated solution. In particular, the National Institute of Standards and Technology has made significant progress in the development of critically important compliance testing programs to implement standards in practice and provide public safety practitioners with performance assurance independent of manufacturer claims.

The long term goal of P–25 is seamless public safety communications interoperability and telecommunications transparency. Achieving that goal is dependent upon leadership, adequate funding and sound planning at all levels of government.

While the P–25 Steering Committee continues to meet and the standards continue to evolve, public safety practitioners continue to purchase communications systems. Because the completion of the P–25 suite of standards continues to be delayed, at

the same time advancements in wireless technology continue, NIJ's CommTech TWG has recommended that NIJ follow a dual path approach: both supporting development of standards in technology beyond P–25 (such as WiFi/802.11x, WiMax/806.16x and VoIP) and continuing to support P–25. We concur with them that the completion of P–25 standards, by itself, will not solve the standards problem.

NIJ's Efforts

Within existing budget constraints, and the myriad of competing technology needs of the criminal justice community, NIJ has been devoting on average $13 million per year to its CommTech portfolio. We are pleased to report that a remarkable amount of work has been done through focusing our investment. In addition to technology assistance, standards development and testing, NIJ has funded approximately 20 research, development and demonstration projects per year.

Among our accomplishments, NIJ funded the development of the Virginia Statewide Communications Interoperability Plan (SCIP), a national model for state-level planning and cooperation. NIJ worked closely with SAFECOM to develop the Virginia SCIP and continues to encourage the use of the SCIP methodology elsewhere in the nation.

One of our most notable accomplishments in the public safety communications technology arena has been funding the development of the Computer Assisted Pre-Coordination Resource and Database System (CAPRAD). This tool aids more than 50 regional planning committees to plan and use regional frequency spectrum efficiently and to better manage potential interference near jurisdictional borders. NIJ also convened a National Task Force on Interoperability and published a guidebook and pamphlet: *Why Can't We Talk* that discussed the need for federal, state and local leadership on interoperability. This publication was developed to facilitate education and discussion among and between elected and appointed officials, their representative associations, and public safety representatives on public safety wireless communications interoperability.

NIJ publishes a wide range of communications-related information for public safety professionals, such as the *Understanding Wireless Guide,* which provides a comprehensive discussion and explanation of communication systems for public safety. NIJ sponsored the development of a satellite link for the Alaska LMR system. This technology will be tested in other rural environments in the coming year under NIJ funding. The benefit of this technology in situations where the local communications infrastructure has been significantly degraded by a manmade or natural disaster is clear. However, its potential to address the more common needs of policing in rural environments with minimal communications infrastructure needs to be explored.

Through CommTech, NIJ was responsible for development of the Metropolitan Interoperability Regional System (MIRS). MIRS is designed to meet the voice communication interoperability needs of the public safety agencies in the Metropolitan Washington, DC region. It is being used extensively by federal, state, and local law enforcement agencies to aid in communication for multiple agencies in high-profile events such as the Presidential Inauguration. The MIRS testbed has produced important national benefits to public safety by improving the understanding of the benefits of communications switching technology and the pitfalls involving effective implementation of such systems.

CommTech pilot programs are unique in leveraging the participation of the vendor community by pairing a vendor with a public safety agency. NIJ partners with local law enforcement agencies and brings a specific technology to evaluate. This maximizes outcomes while simultaneously minimizing costs to the federal government. For example, NIJ is conducting a pilot program in VOIP in Danville, VA. NIJ is also exploring opportunities to initiate new pilots with SDR and wireless broadband technologies.

A major part of the CommTech program is technology test and evaluation to provide unbiased information to the public safety community. NIJ serves as an independent evaluator, trusted partner, and honest broker. These evaluations also serve to point out technology gaps that need to be filled through further research and development. NIJ has administered standards-based testing programs for criminal justice practitioners for nearly 30 years, such as its body armor testing program. Because of NIJ's body armor standard, officers have confidence in the protection afforded by their personal protective equipment. Over 3,000 officers' lives have been saved by NIJ-compliant body armor.

Public safety officials are making communications purchase decisions every day and assistance to evaluate the rapidly changing communications landscape. NIJ provides this in many ways including through our web site and publications such as the *Why Can't We Talk* guidebook and pamphlet, and our Technology In-Shorts documents.

NIJ also actively responds to technology assistance requests that we receive from public safety officials across the country. In just the last two weeks, we have responded to a request to assist with development of a communications system in Katrina-affected Mississippi and Louisiana; a technology assistance request in Haverhill, MA; and participated in a meeting with San Joaquin, CA officials concerning communications needs. Last week, a captain of the Alexandria Police Department and a member of the CommTech team, along with staff from the National Law Enforcement and Corrections Technology Center- Southeast started to work with the Fredericksburg, VA Police and Fire Chiefs to establish interoperable communications via an interconnect switch and are addressing ways in which to optimize coverage without significant financial investment. Through the Sheriff's Association of Texas (SAT), NIJ has active and ongoing technology assistance requests with 26 Brazoria County fire departments; Frio County, Webb County, Medina County, Caldwell County, and El Paso County Sheriff's offices; and the Middle Rio Grande Development Council of Governments. NIJ is also working with SAT to further develop communications operability and interoperability for state and local agencies along the entire 26 county US-Mexico border.

CommTech provides technical support to tactical operations. CommTech provided interoperability assistance in both the 2001 and 2005 Presidential Inaugurations, Hurricane Rita response, the dedication of the World War II Memorial, and the Moussaoui trial. In May 2006, the CommTech Program will provide interoperability support for the opening ceremonies for the Woodrow Wilson Bridge via the development of an interoperability plan.

NIJ provides a critical resource to other components of DOJ related to interoperability. NIJ works very closely with the COPS Office to support their grants review process. NIJ helped to fund the DOJ Interoperability Summit in Seattle in May, 2005 and will do so again in Austin next month (May 2006). NIJ has arranged for active sworn state and local law enforcement personnel, as well as interoperability technical experts, to support all of our federal partners in interoperability efforts.

Assistance to State and Local Practitioners

NIJ's National Law Enforcement and Corrections Technology Center (NLECTC) system offers public safety agencies, both large and small, no-cost assistance in the implementation of current and emerging technologies. With a network of ten regional centers and specialty offices located across the country, the NLECTC system delivers expertise in a number of technologies including communication interoperability and information sharing. The NLECTC system plays a vital role in NIJ's CommTech efforts.

The staff of the NLECTC system's Western Center (NLECTC-West) has supported CommTech by providing subject matter experts in the field of SDR. Also, Pima County Arizona asked NLECTC-West for technology assistance in developing a communication network. The various agencies in the county use different radio systems making mutual aide interoperability difficult or impossible. Additionally, radio coverage is poor due to the mountainous terrain. NLECTC-West drafted a technical requirements document for that communication system.

The NLECTC system's Rocky Mountain Center houses the previously discussed CAPRAD database, which allows all 55 regional planning committees (RPC) to have access to tools to coordinate their frequency planning. The RPCs also provide feedback on the CAPRAD system for continuing improvement.

Conclusion

The goal of improving public safety communications interoperability can only be achieved by dealing with the overall problem of operability. Focusing on interoperability as the only issue in first responder communications will not yield a result that will allow the responder to communicate or access information effectively.

NIJ has, at the recommendation of its practitioner-driven TWG, focused on many aspects of first responder communication operability, including interoperability. With the support of the FCC, NIJ has funded Regional Planning Councils to address local spectrum issues. It has supported the development of CAPRAD to monitor and track first responder spectrum requirements and usage across the U.S. We have supported fundamental R&D in SDR and cognitive radios in order to address issues of operability as much as interoperability. We have worked closely with the vendor community to test and evaluate the products in a real world environment and NIJ provides ongoing technology assistance through our NLECTC system.

Today, there are fundamental challenges to operability. SDR and cognitive radio technologies offer the promise to enhance communications capabilities within the current available spectrum allocations. Although new spectrum from the digital television transition will help, new technologies can help public safety to improve operability and interoperability for years to come. A single entity, or even the entire fed-

eral government, will not solve the interoperability challenge alone. There is overlap between the activities of the various federal partners for interoperability. Each represents a constituency with common as well as unique needs. Clearer delineation and better coordination among federal entities with respect to interoperability is what all of the agencies are striving to achieve. Although the challenges in public safety communications will take many years to solve, the federal government can best play a role by working towards the establishment of a comprehensive, coordinated, standards-based strategy.

Mr. REICHERT. Thank you. The Chair recognizes Mr. Orr.

STATEMENT OF DERECK ORR, PROGRAM MANAGER, PUBLIC SAFETY COMMUNICATIONS SYSTEMS, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Mr. ORR. Thank you, Mr. Chairman. I am sincerely honored to be here this morning with you and the esteemed members of the subcommittee. This public safety communication program serves as the technical lead for several of the administration's initiatives focusing on communications, including SAFECOM and the COPS office, and although NIST is helping to improve public safety communications through a number of efforts, many of which other panelists have spoken of, I will focus the remainder of my remarks on the state of standards for public safety communications systems.

Interoperability for public safety communications is defined as the ability to share information via voice and data on demand, in real time, when needed and as authorized. The public safety community expects this level of interoperability will be available using equipment from multiple manufacturers, be transparent to the user, require little or no special knowledge of the system and not be dependent on common frequency assignments. Obviously this is not what we have today.

Achieving this definition of interoperability in the future will not be possible without the existence of standards. Of course, public safety radio users have recognized this for some time. Approximately 15 years ago representatives from local, state and federal agencies joined together to address the absence of available standards. They did this for two primary purposes. First was to ensure the interoperability could be achieved assuming the use of equipment from multiple manufacturers. Second, through standards, the public safety community wanted to be able to take advantage of cost reductions associated with the more competitive land mobile environment.

The public safety community in the form of a P25 steering committee partnered with the Telecommunications Industry Association, TIA, to serve as the standards development organization for this effort. Thus, Project 25 or P25 as we know it today, was launched. A commonly misunderstood aspect is that it is comprised of a single standard. Instead, it is a suite of standards that specify the eight interfaces between the various components of a land mobile radio system. Handheld to handheld, handheld to mobile unit, mobile unit to tower.

Until this past January, the last years had resulted in only one of the P25 interfaces, the common air interface that deals with the functions of the handheld units; i.e., the walkie-talkies, being advanced to a level where it would help satisfy one or both of the goals of P25. However, over the last year through the concerted ef-

forts of industry, public safety practitioners and NIST and its federal partners, with the support of SAFECOM, the technical development of standards for the critical P25 interfaces has been greatly accelerated.

Industry representatives with key involvement, like public safety practitioners, have dramatically increased the pace and scope of their standards development activities consistent with the priorities set by Congress. As a result, significant progress has been made through the formal standards development framework established by the P25 TIA partnership in 1993.

Specifically, the most critical P25 radio system interfaces have all been addressed. Basic protocol standards that specify the functionality and capability of those interfaces have been completed and have been or are on the verge of being published. Adoption of P25 standards is now occurring within a timeframe acceptable to public users, NIST, and manufacturers.

As of the March 2006 P25 meetings, the following has occurred: The Fixed Station Interface standard has been approved for publication as a TIA standard. The Fixed Station Interface standard also serves as a Basic Console Interface standard. The Inter-RF Subsystem Interface, ISSI, a key standard for interoperability, is in final stages of balloting and is expected to be approved by TIA during a May 1st P25 meeting.

I can report that state and local public safety agencies are already referencing the above standards in formal requests for proposals to industry and that manufacturers are in the process of building these standards into future land mobile radio product lines. In addition, Mr. Chairman, over the last 2 years NIST, with funds from the Department of Homeland Security and Justice, has tested a number of the handheld P25 radios that claim to meet the widely available Common Air Interface standard. Using the test procedures called for in the standards, NIST found none of the available radios met all aspects of the standard.

Therefore, NIST, with the support of SAFECOM and the P25 steering committee, is developing a P25 Compliance Assessment Program. NIST is preparing and documenting standardized test protocols for the most important aspects of the Common Air Interface standard. The standardized test protocols will be provided to NIST's National Voluntary Laboratory Accreditation Program, which can accredit laboratories across the country interested in offering these testing capabilities. These will go a long way in assuring the community that the equipment being purchased meets the P25 standard.

In summation, Mr. Chairman, there are positive steps being taken by leaders in the community, key Federal programs, the Congress and industry to significantly change the current environment and move the state of standards for public safety forward. By the end of May, there will be newly adopted P25 standards covering three additional key interfaces which can be tied to grants and procurements. By the end of this calendar year, radio users will have a mechanism in place to ensure the products they are purchasing do what is called for in the applicable standards.

Again, I am honored to be here before this committee today and I am happy answer any questions you may have.

[The statement of Mr. Orr follows:]

PREPARED STATEMENT OF DERECK ORR

APRIL 25, 2006

Thank you Chairman Reichert and Members of the Committee, I serve as the Program Manager for Public Safety Communications Systems in the Office of Law Enforcement Standards at the National Institute of Standards and Technology (NIST). NIST a non-regulatory agency within the U.S. Commerce Department's Technology Administration serves industry, academia, and other parts of the government by promoting U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

NIST's public safety communications program serves as the technical lead for several Administration initiatives focusing on communications, most importantly the SAFECOM Program. NIST is involved in many of the key SAFECOM initiatives, including the Statement of Requirements, Public Safety Architecture Framework, testing and evaluation, and standards development. The strong partnership between SAFECOM and NIST is an excellent example within the Administration of multi-agency coordination and collaboration, and is something for which we at NIST are very proud. In addition, NIST relies heavily on the world-class engineering expertise of the Institute of Telecommunications Sciences within NTIA.

I will focus the remainder of my remarks this morning on the state of standards for public safety communications systems.

Interoperability for public safety communications is defined as "the ability to share information via voice and data signals on demand, in real time, when needed, and as authorized." The public safety community expects that this level of interoperability will be available using equipment from multiple manufacturers, that they are transparent to the user, requiring little or no special knowledge of the system, and that they are not dependent on common frequency assignments.

Achieving this definition of interoperability is not possible without the existence of standards that will define how the various components of a public safety communications system will interoperate, regardless of manufacturer. In fact, I would venture to say that in the absence of standards, achieving this level of interoperability would not be possible.

Public safety users have recognized this for some time. Approximately fifteen years ago, representatives from local, state, and federal public safety associations and agencies joined together to address the absence of available standards. They did this for two primary purposes. First was to ensure that interoperability could be achieved, assuming the use of equipment from multiple manufacturers. Second, through standards, the public safety community wanted to be able to take advantage of cost reductions associated with a more competitive land mobile radio market.

Understanding the difficulty in specifying the complex operations of the various components of a land mobile radio system, the public safety community partnered with the Telecommunications Industry Association (TIA) to serve as the standards development organization (SDO) for this effort. Thus Project 25, or P25 as we know it today, was launched. A Memorandum of Understanding formalizing this relationship created a Steering Committee comprised only of public safety and government representatives and invested the committee with the sole authority to designate a P25 standard.

A commonly misunderstood aspect of P25 is that it is comprised of a single standard. Instead, it is a suite of standards that specify the eight interfaces between the various components of a land mobile radio system (hand held to hand held, hand held to mobile unit, mobile unit to repeater, etc.):

- Common air interface: this interface defines the wireless access between mobile and portable radios and between the subscriber (portable and mobile) radios and the fixed or base station radios;
- Subscriber data peripheral interface: this interface characterizes the signaling for data transfer that must take place between the subscriber radios and the data devices that may be connected to the subscriber radio;
- Fixed station interface: this interface describes the signaling and messages between the RFSS and the fixed station by defining the voice and data packets (that are sent from/to the subscriber(s) over the common air interface) and all of the command and control messages used to administer the fixed station as well as the subscribers that are communicating through the fixed station;
- Console interface: this interface is similar to the fixed station interface but it defines all the signaling and messages between the RFSS and the console,

the position that a dispatcher or a supervisor would occupy to provide commands and support to the personnel in the field;

• Network management interface: this interface to the RFSS allows administrators to control and monitor network fault management and network performance management.

• Data network interface: this interface describes the RF subsystem's connections to computers, data networks, external data sources, etc.;

• Telephone interconnect interface: this interface between the RFSS and the Public Switched Telephone Network (PSTN) allows field personnel to make connections through the public switched telephone network by using their radios rather than using cellular telephones;

• Inter RF subsystem interface: this interface permits users in one system to communicate with users in a different system, from one jurisdiction to another, from one agency to another, from one city to another, etc.

Until this past January, the last fifteen years had resulted in only one of the above P25 interfaces, the Common Air Interface that deals with the functions of the hand held units (i.e., walky-talky), being advanced to a level where it would help satisfy one or both of the goals of P25. The remainder of the interfaces had either remained undefined, or lacked enough specificity to allow for a common implementation of the interface; in other words each manufacturers implementation of the interface would be different and proprietary thus resulting in systems that would not meet the "interoperability" requirements as defined by the steering committee.

I would like to emphasize that the Common Air Interface was a major step forward and extremely important. It provides a level of interoperability and competition in the hand-held market that was not available before. But, it alone cannot satisfy the definition of interoperability that the public safety community is calling for.

However, over the last year, through the concerted efforts of industry, public safety practitioners, and NIST, with the support of SAFECOM, the technical development of standards for the critical P25 interfaces has been greatly accelerated. Industry representatives, with key involvement by public safety practitioners, have dramatically increased the pace and scope of their standards development activities consistent with priorities set by Congress. As a result, significant progress has been made through the formal P25/Telecommunications Industry Association (TIA) standards development framework established by the P25/TIA partnership in 1993. Specifically, **the most critical P25 radio system interfaces have all been addressed.** Basic protocol standards that specify the functionality and capability of these interfaces have now been completed and have been, or are on the verge of being published. The adoption of P25 standards is now occurring within a time frame acceptable to public safety users, NIST and its Federal partners, and the manufacturers.

As of the March 2006 P25 meetings the following has been achieved to add to the existing P25 Common Air Interface:

• **Inter-RF Subsystem Interface (ISSI):** A draft ISSI standard was approved on January 11, 2006 for letter balloting as a TIA standard. TIA anticipates that the vote for publication will occur during a formal meeting on May 31, 2006. The public safety community can expect ISSI products to be available in 2007 (within approximately six months after publication of relevant standards in 2006 consistent with deadlines established by the P25 Steering Committee

• **Fixed/Base Station Subsystem Interface (FSSI):** A completed FSSI standard was approved on January 11, 2006 for publication as a TIA standard. The realization of a TIA standard for the FSSI is extremely important because this standard will result in the offering and procurement of interoperable multi-vendor equipment enabling direct control by the console and Radio Frequency Subsystem (RFSS) of fixed/base station equipment. The console functionality provided by the FSSI substantially mitigates the urgency for completion of the CSSI. The public safety community can expect FSSI products to be available in late 2006 (within approximately six months after publication of relevant standards in 2006 consistent with deadlines established by the P25 Steering Committee).

• **Console Subsystem Interface (CSSI):** Completion in January 2006 of a new TIA standard for the FSSI that enables direct basic console control of fixed/base station equipment now serves as the foundation for more comprehensive CSSI standards to be developed in the future. Further development of the CSSI will follow upon continued development of the ISSI and FSSI throughout calendar year 2006. The public safety community can expect CSSI products to be available in 2007 (within approximately six months after publication of relevant standards in 2006 consistent with deadlines established by the P25 Steering Committee).

I can report that State and local public safety agencies are already referencing the above standards in formal requests for proposals (RFPs) to Industry and that manufacturers are in the process of adding these standards to future land mobile radio product lines.

Of course, it is not only important that the various P25 interfaces are completed in a timely manner, but that a mechanism exist to ensure that products built to the standard, meet all of the requirements of the standard. Over the last two years, NIST, with funds from the Department of Homeland Security and the Department of Justice, has tested a number of the hand held P25 radios that claim to meet the available Common Air Interface Standard. Using the test procedures called for in the standard, NIST found that none of the available radios met all aspects of the standard.

As with many other standards developed through the private sector consensus process, the key to correct adoption and implementation by different manufacturers is a strong conformity assessment program. A conformity assessment program will validate P25 standardized systems through a set of agreed upon tests which will validate that the systems can interoperate among themselves, thus ensuring Federal grant dollars are being used appropriately. NIST, with the support of SAFECOM and the P25 Steering Committee, is developing a P25 Conformity Assessment Program. NIST is preparing and documenting standardized test protocols for the most important aspects of the Common Air Interface Standard. The standardized test protocols will then be provided to NIST's National Voluntary Laboratory Accreditation Program (NVLAP), which can accredit laboratories interested in offering these testing capabilities. These test protocols would go a long way in assuring the public safety community that the equipment being purchased meets the P25 standard.

NIST is working closely with the P25 Steering Committee and manufacturers to ensure that the test procedures are correct and that the results are accurate. In addition, not all aspects of the P25 common air interface will be immediately available for testing through this program. To begin with, NIST is focusing on some basic functional tests of the radios, which will allow us to get the Compliance Assessment Program up and running. We will then begin to add interoperability tests, as well as tests for more complex radio functions.

In summation Mr. Chairman, there are positive steps being taken by leaders within the public safety community, key federal programs, the Congress and industry to significantly change the current environment and move the state of standards for public safety forward. The last twelve months have seen significant progress in the development of critical P25 standards and the next twelve months will see even more progress made., In addition, by the end of this year, local, state, and federal agencies procuring P25 equipment will have a mechanism in place to ensure that the products they are purchasing truly do what is called for in the applicable standard. In conjunction with the other efforts mentioned by the other witnesses, I am confident that we are making significant headway in the pursuit of communications interoperability.

NIST looks forward to working with this Committee, Congress, our federal partners, state and local public safety officials, and leaders in industry to make this happen. Again, I am honored to be here before this Committee today, and I will happy to answer any questions that you may have.

Mr. REICHERT. Thank you. Mr. Gass is recognized.

STATEMENT OF JAMES GASS, DEPUTY DIRECTOR, NATIONAL MEMORIAL INSTITUTE FOR THE PREVENTION OF TERRORISM

Mr. GASS. Mr. Chairman, distinguished members of the committee, my name is Jim Gass and I am the Deputy Director of the National Memorial Institute for Prevention of Terrorism, MIPT for short. I have been there about 5 years, and I am also a member of the Interagency Board for Equipment Standardization and Interoperability and also have been for 5 years.

Just a quick note on MIPT by way of background. We are the third component of the memorialization process that grew out of the Oklahoma City bombing, and it was the desire of the citizens that there be some institute that would be in the proactive business of developing technologies, and so forth, that would assist the

responders either to prevent or better mitigate against terrorism, and we are grateful to Congress for our earlier appropriations. Those appropriations flowed through, interestingly, the Office of Science and Technology, NIJ, DOJ, and Dr. Boyd was our original Federal monitor.

In that original appropriations language we were instructed among other things to conduct counterterrorism research and development, build Internet accessible best practices and lessons learned systems and institute a pilot project to develop a research development test and evaluation program similar to the Department of Defense systems. That guidance and our focus on emergency responders led us to create something called Project Responder, which given the threat from CBRNE we asked the full spectrum of responder disciplines what kinds of capabilities they needed, compared those needs to existing and emerging technologies, trying to discover where there were gaps in the research and development agenda.

That project produced a national technology plan for emergency response to catastrophic terrorism. There was a complete section of that report devoted to, quote, unified incident command support and interoperable communications. I will draw some of my remarks from that study.

A key finding of Project Responder was that technology already existed to achieve interoperable communications and concluded, quote, organizational changes, equipment/interface standards and practice/training may be more relevant than technology in solving some of the problems.

Two years ago MIPT launched the Lessons Learned Information and Sharing System, LLIS.gov. In a quick review through that database, it is obvious that we have had problems with interoperable communications in just about every major terrorist incident and national disaster. There were communication problems in Oklahoma City, the World Trade Center, the Pentagon and of course Hurricane Katrina.

Because of the Air Florida crash some years earlier, the Washington Metro area diligently worked to buy interoperable communications and had jointly practiced using them. So in some degree they were well ahead of a lot of the communities. And to the degree that the responders to the Pentagon were from that mutual aid area, it worked pretty well. The problem was more with the myriad of other responders that were not part of that habitual group. Of course Katrina was a different animal. It actually decapitated the local infrastructure, with much of it under water.

So with all that background, why haven't we fixed the problem? I am speaking now as someone non-federal and outside the Beltway and with the perspective of having talked to responders and having absorbed with their concerns are. I believe the components to fixing the problem falls into five categories: National policies and strategies; frequency spectrum; national standards; a common operating picture; and resources for replacing/augmenting legacy systems.

First, we need a national vision and strategy to achieve it. Jurisdictions buy equipment based on their own needs and resources. Without an overarching strategy we will keep doing what we are

doing, and that may not contribute to a national interoperable plan.

Second, there is the issue of frequency spectrum. Although Congress recently passed legislation that will allow access to the 700 megahertz spectrum, there will still be competition over how much and what parts to dedicate to the emergency response community. Access to that part of the spectrum is still 3 years away.

Third, there is a lack of standards for interoperable communications. Progress is being made but it is painfully slow. By the way, I believe that standards must include not only technical elements but must also ensure that we have the necessary test procedures and protocols in place to allow for third party testing and certification. NIST is also working on that.

We insist on certification testing for our responder personal protective equipment. We should do no less for the communications equipment. I think SAFECOM also advocates that and is pushing that as well.

Fourth, we need to think about how to establish a common operating picture. I mentioned I was in the Army for 30 years. We always had—we had a set of what we called signal operating instructions, SOIs, which enabled everybody who came into an area of operations to know who to call and on what frequency based on their level of command and function. While it may be desirable to have the capability for everybody to be able to talk to everyone else, that would be chaotic and not how we would want to operate. We should predetermine who should talk to whom and provide the information about how to do that in advance of an incident.

Fifth, and after we have all of the above we will have to deal with the issue of phasing out all of the legacy systems. With the millions of communications systems in existence today, we will have to go about that smartly or we may spend enormous amounts of resources. There already exists several bridging/gateway technologies that can help us through that phase into standards-compliant communications systems.

In summary, we believe that the real challenge here is not about new technology, it is about Federal leadership and providing interference-free spectrum, clear standards with real certification for equipment, and assistance in developing effective communications plans and incident management processes.

Mr. Chairman, this concludes my remarks. I am happy to answer any questions.

[The statement of Mr. Gass follows:]

PREPARED STATEMENT OF JAMES M. GASS

Mr. Chairman, and distinguished members of the committee, my name is Jim Gass and I thank you for this opportunity to appear before you. I am the Deputy Director of the National Memorial Institute for the Prevention of Terrorism (MIPT) in Oklahoma City and have been with MIPT for more than five years. Prior to joining MIPT, I served 30 years in the United States Army.

MIPT is the third component of the Memorial of the bombing of the Alfred P. Murrah Federal Building, April19, 1995. It was created in response to the victims', family members', responders' and citizens' desires to have an Institute dedicated to proactive efforts to prevent terrorism or better mitigate its effects.

Since our inception, our primary focus has been on projects to improve the preparedness of emergency responders. We are grateful to Congress for originally supporting us with appropriations in our early years. Initially, our awards were made through the National Institute of Justice, Department of Justice, but with the for-

mation of the Department of Homeland Security, we have received additional discretionary awards to continue our programs.

Language in some of our earlier Congressional Appropriations Bills charged us with doing a number of things. I would like to restate a few of those because they provide some underpinning to my remarks about the critically important subject this committee is hearing today. These bills instructed us to conduct counterterrorism research and development; create an Internet repository where emergency responders can share best practices, observations, and lessons learned; and to institute a pilot project to develop an RDT&E system similar to the Department of Defense System.

This guidance and our desire to focus our own research agenda on emergency responders, led us to conduct an effort we called Project Responder which produced a report titled "National Technology Plan for Emergency Response to Catastrophic Terrorism. Project Responder evaluated needed capabilities as stated by the responders themselves, studied the state of current technology and provided information that could help inform federal and private sector research and development agendas. Unified Incident Command Decision Support and Interoperable Communications was a significant part of the capabilities needed by responders. In addition to the clear increases in capability that interoperable communications would provide, many other highly desired and needed functional capabilities could be enabled by interoperable communications. These functional capabilities are currently not available, but could be achievable at low technological risk. These include 1) point location and identification to help incident commanders know where their personnel and equipment are at any given time, 2) seamless connectivity to aid when multiple agencies and jurisdictions work together at a site, and 3) information assurance to ensure the availability of information, as well as what is communicated, not be compromised by adversaries during a crisis. Providing command information and dissemination tools and multimedia functional capabilities were also identified by Project Responder, but were not as highly prioritized as the previous three. One of our key findings was that technology already exists to achieve interoperable communications. New research and development into communications technologies is not needed to solve interoperability. Instead Project Responder concluded that "organizational changes, equipment/interface standards, and practice/training may be more relevant than technology in solving some of the problems." I will return to these points later in my testimony.

I welcome the opportunity to talk to you today about the issue of communications interoperability and its importance to the response community. The ability to communicate is essential for local emergency responders and the State and Federal officials who assist them. But too often in major disasters our ability to communicate with one another has been impaired. At Oklahoma City in 1995, at the World Trade Center and the Pentagon on September 11, 2001, and in the countless other emergencies that our emergency responders face everyday, communications interoperability problems not only make their jobs more difficult, but risk the lives of the both victims and responders.

Unfortunately, these are not new problems. One of MIPT's most important goals is to promote the sharing of lessons learned and best practices within the emergency response community. Two years ago MIPT launched the *Lessons Learned Information Sharing (LLIS.gov)* system, the national network for lessons learned and best practices. A quick glance on LLIS.gov shows several lessons learned related to communications interoperability. For example, during the response to the attack on the Pentagon in 2001, mutual aid personnel arrived at the scene with radios that could not communicate—or easily be reprogrammed—with either the Arlington County Fire or Police Departments. And the DC Metro area was probably years ahead of most jurisdictions in moving toward interoperability. With the communications system, technical personnel, and cellular phone networks quickly overloaded during the initial response to the World Trade Center attacks, emergency responders were forced to rely on foot messengers to communicate during the first few hours of operations.

The response to Hurricane Katrina further highlighted communications interoperability as a significant problem in the response—at the Federal, State, and local level. The after-action report *The Federal Response to Hurricane Katrina—Lessons Learned* concludes that communication plans and assets were neither sufficient nor adequately integrated to respond effectively to the disaster. Many available communications assets were not utilized fully because there was no National, State-wide, or regional communications plan to incorporate them. Officials from national leaders to emergency responders on the ground lacked a common interoperable communications infrastructure to provide the necessary situational awareness so critical to a prompt and effective response. The Select Bipartisan Committee to Investigate the

Preparation for and Response to Hurricane Katrina found that "issues with interoperability among Federal, state, and local communications systems complicated the efforts of first responders and government officials to work together in managing the response to Katrina."

Because communications problems have appeared as a "lessons learned" in almost every major terrorism event or major natural disaster, why haven't we fixed it? It's because some of the components of fixing it are incredibly complex and incredibly expensive. I believe the components of the fix falls into five categories: (1) National Policies and Strategies; (2) National Standards; (3) Frequency spectrum; (4) Resources for replacing legacy systems; and (5) a common operating picture.

Let me give a brief discussion of each:

First, I believe that we must, as a nation, develop a set of comprehensive policies or strategies that lay out a national interoperable communications vision. Jurisdictions across the country follow their own guidelines regarding communications systems and equipment based upon their own resources and needs. Some areas of the country have established regional or state communications systems that link State and local agencies. But Federal policies and strategies are needed to guide decision makers at all levels of to strive for a national solution to the interoperability problem.

Second, there is also a lack of national standards for interoperable communications. A recent report released by Inspector General of the Department of Homeland Security found that no new standards have been issued since February 2004. National interoperable communications standards must be developed in order to provide guidance to state and local jurisdictions on acceptable and required equipment and systems. The Responder Knowledge Base, another key MIPT program, provides information on adopted equipment standards and certifications to the emergency response community and will quickly disseminate information on new interoperable communications standards as it becomes available. There is work underway to develop these standards called P25, but there are complex issues associated with that effort. The constant advances in technology make this a moving target. Just imagine that if ten years ago, we had decided to assign national standard to computers. We might well have been stuck in the 286 mode instead of Pentium 2 or 3. Having said that, it still is not an excuse for not setting a minimum standard to meet emergency response interoperability needs based on currently available technology knowing that in a few years (or months) you may have adjust them based on the advances. And, I believe that we must insist on independent third party testing to assure compliance with the standards.

Third, we must, as a nation, decide how much and in which frequency spectrums we need to give exclusive domain to the emergency response community. It is my understanding that we have a good idea about that, but those spectrums are currently occupied and buying out the spectrum to dedicate to emergency response is both a legal and expensive problem. I'm not an expert on that but I have read that the figure to buy out spectrum short of current agreements is in the billions.

Forth, and only after we have national standards, we must consider the amount of resources that would be required to replace all of the non-compliant communications in the nation and who should pay. Most communications capability resident in the local jurisdictions have been purchased with local dollars and designed to meet local needs as best envisioned by local leaders. Once we have national standards, how do we phase out the old and phase in the new. I don't know the exact number of communications devices there are in the nation, but if we have upwards of 8,000,000 responders and even half of them are equipped with communication equipment, replacing them all would be a staggering amount and doesn't answer the question about who would have the primary responsibility for the cost burden—Federal, state or local? Jurisdictions across the country do not have the resources available to do an immediate upgrade to existing systems and equipment. Project Responder found that "jurisdictions have existing radios and support tower infrastructure and do not have the money to upgrade them". Once we have national standards and certification testing, I have to believe that when new equipment is purchased, even with local money, jurisdictions would go in the direction of standards compliant equipment.

Fifth, I believe we must procedurally standardize how and with whom we must communicate. This is definitely not a technology issue—it is a procedures issue. Even if we had perfect ability for everybody to communicate with everybody else, it doesn?t mean that is how we would want to operate. We must determine in advance who needs to talk to whom and provide them with the information about how to link their communications based on the function(s) being performed. I mentioned that I came from an Army background. We used to have Signal Operating Instructions (SOIs) which provided all the players in the area of operations predetermined

information about how to contact other people based on the levels of command and functions being performed. These SOIs contained the frequencies and call signs of all of the participants who might enter the area of operations. No one had to search for information about how to contact the appropriate people to engage their capabilities. As the National Response Plan, the National Incident Management System and mutual aid agreements mature and are practiced, this process will become clearer. But it is one of the reasons Project Responder suggested that "organizational changes, equipment/interface standard and practice/training may be more relevant than technology in solving some of the problems."

Mr. Chairman, this concludes my written statement. I am happy to answer any questions that you or the members of the subcommittee may have.

Mr. REICHERT. Thank you very much. Mr. Walker is recognized.

STATEMENT OF BRUCE WALKER, CHAIRMAN, SUBCOMMITTEE ON GOVERNMENT AFFAIRS, HOMELAND SECURITY AND DEFENSE BUSINESS COUNCIL

Mr. WALKER. Good afternoon, Chairman Reichert, Ranking Member Pascrell, and distinguished members of this subcommittee. My name is Bruce Walker and I work for Northrop Grumman Corporation. Today I am testifying on behalf of the Homeland Security Defense Business Council and our 30-plus member companies. I serve as the Chair of the Government Relations Committee and have had the privilege of delivering and developing a number of Homeland Security topical briefings to the committee staff over the last year.

The Homeland Security Defense Business Council is a nonprofit, nonpartisan organization that represents good governance and successful program outcomes in the Homeland Security marketplace. The Council offers straight talk and honest assessments of programs, technologies and processes integral to the mission of the Department of Homeland Security. The Council's goal is to be a world class private sector component and partner to the public sector in all significant areas of homeland security, to include risk mitigation, mission effectiveness and management efficiency.

The Council appreciates the opportunity to present our industry perspective on the state of interoperable communications today. I would like to begin with a brief summary of the Council's recommendations to Congress.

First, in order to get it right, interoperability is more than just technology. It is standards and money. Federal, State, local, tribal and even private sector participants also need to deal with business process changes and user training issues and the long-term investment model changes required to successfully leverage interoperability.

While we are talking about leverage, interoperability is really about leverage. Applying interoperable communications to today's safety and first responder communities opens the aperture to new applications in technologies and voice, data and video. These need to be designed to deliver higher value, tactically significant information at the point where it is going to do the most good.

Third, we believe that more emphasis needs to be placed on the governance layer of the SAFECOM interoperability continuum. The focus has been centered around technical and spectrum issues. More engagement of the practitioner community for developing practical models is something we need to do to address the real issues of multiplayer interoperability.

Finally, we believe there needs to be more complete engagement of industry, especially national players in DOD systems, where RDT&E programs eligible for inclusion in the DOD 1401 Technology Transfer Program can be used to address SAFECOM initiatives.

For many public safety organizations interoperability is best seen from a cost and timeline perspective. The more affluent organizations have access to current generation capabilities at a faster pace and are able to deploy and sustain systems that leverage flexible spectrum use and more efficient use for weight and power usage. Those with more modest budgets extend existing systems as far as possible in order to delay the need to reinvest. Yet, the costs of sustaining the legacy environment increase every year and reinvestment becomes more and more difficult to achieve.

One of the core difficulties occurs when communities need coordinated responses from organizations on either end of this budget reality. The 2004 release of the SAFECOM statement of requirements for wireless public safety communications interoperability established the structure, explained the need, and describes the future operational model for everyone to shoot for. Certainly all good things, but the practical funding reality makes this a very challenging objective.

What is missing is guidance and governance on how to get there. Budget formulation options, grant applications support, business process, training and operation overhauls are all needed services in order to make SAFECOM's vision a reality at the national level. Private industry also needs to be included in the picture.

Clearly it makes sense to apply resources and funding in urban areas where the threat is the highest. But ignoring the need to upgrade, integrate and train rural and remote communities moves the SAFECOM vision to the right. Small border state communities and internal communities alike need to interoperate with their urban counterparts, particularly in situations where regional response capabilities are stretched beyond the breaking point.

The SAFECOM SoR provides need direction to the challenge. It gives both government and industry access to the leverage mentioned in the second of our recommendations. Industry directly benefits from the SoR because it allows us to design critical research and development efforts with interoperable demand.

Public safety and other first responder organizations benefit from the establishment of a standards baseline upon which they can base sourcing and selection decisions. Clearly these are again all good things but the real measure of success will be in the integration and the deployment of new capabilities directly addressing new threats of terrorism and old threats, like national disasters.

The new application horizons that interoperability offers are critical components in ensuring the safety and security of our country. The ability to provide integrated command and control across multiple responders with different technology baselines or the ability to locate first and then dispatch critical resources and material to specific locations will make huge differences in our ability to respond to potentially disastrous events. These applications come from many sources, not the least of which is DOD, and aggressive reuse of technologies developed to support our troops in foreign

operational theaters. They need to be accelerated wherever appropriate because the investment in R&D has already been made. Public safety and first responder environments are not the same as foreign operational theaters and solutions need to be carefully vetted to make sure they are used as well as any unintended consequences of their use meet our laws and fit business and operational needs of the user community.

That concludes the remarks I have today, sir. Glad to answer any questions.

[The statement of Mr. Walker follows:]

PREPARED STATEMENT OF BRUCE V. WALKER

APRIL 25, 2006

Good afternoon, Chairman Reichert, Ranking Member Pascrell, and distinguished members of the subcommittee. My name is Bruce Walker and I am with Northrop Grumman Corporation. Today I am testifying on behalf of the Homeland Security and Business Council and our 30+ member companies. I serve as the Chair of our Government Relations Committee and have had the privilege of developing and delivering a number of topical briefings to the Committee? staff over the last year.

The Homeland Security & Defense Business Council is a non-profit, non-partisan organization that represents good governance and successful program outcomes. The Council offers "straight talk" and honest assessments of programs, technology, and processes that are integral to the mission of the Department of Homeland Security. The Council's goal is to be a world class private sector component and partner to the public sector in all significant areas of homeland security to include risk mitigation, mission effectiveness, and management efficiency.

The Council appreciates the opportunity to present our industry perspective on the state of interoperable communications.

Let me begin with a brief summary of the Council's recommendations to Congress:

(1) In order to "get it right", interoperability is more than technology, standards and money. Federal, state, local and tribal governments as well as the private sector also need to deal with the business process changes, end-user training issues, and the long term investment model changes required to successfully leverage interoperability.

(2) Interoperability is also about leverage. Applying interoperable communications to today's public safety and first responder communities opens the aperture for new technologies—voice, data, video—and new applications designed to deliver higher value, tactically significant information at the point where it will do the most good.

(3) We believe that more emphasis needs to be placed on the "governance" layer of the SAFECOM Interoperability Continuum. Although the focus on the various interoperability initiatives has been centered around technical and spectrum issues, more engagement of the practitioner community for developing practical and effective governance models is something that we need to do to address that real issues of multi-player interoperability.

(4) Finally, we believe there needs to be more complete engagement of industry, especially national players in DoD systems, where RDT&E programs eligible for inclusion in the DoD 1401 Technology Transfer program can be used to address SAFECOM initiatives.

For many public safety organizations, interoperability is best seen from a cost and timeline perspective. The more affluent organizations have access to current generation capabilities at a faster pace and are able to deploy and sustain systems that leverage flexible spectrum use and more efficient designs for weight and power usage. Those with more modest budgets extend existing systems as far as possible in order to delay the need to reinvest—yet the costs of sustaining the legacy environment increase every year and reinvestment becomes more and more difficult to achieve.

One of the core difficulties with this model occurs when communities need coordinated responses from organizations on either end of this budget reality. The 2004 release of the SAFECOM Statement of Requirements (SoR) for Wireless Public Safety Communications and Interoperability, established the structure, explained the need, and describes a future operational model for everyone to shoot for—certainly, all good things—but the practical funding reality makes this a very challenging objective. What is missing is guidance and governance on how to get there. Budget

formulation options, grant application support, business process reengineering support, training and operations overhauls—are all needed services in order to make the SAFECOM vision a reality at a national level. Private industry also needs to be included in the picture—particularly in relation to the critical infrastructure under their control and management.

Clearly it make sense to apply resources and funding in urban areas where the threat is the highest, but ignoring the need to upgrade, integrate and train rural and remote communities just moves the SAFECOM vision to right. Small border state communities and internal communities, alike, need to interoperate with their urban counterparts—particularly in situations where regional response capabilities (i.e., Katrina) are stretched beyond the breaking point.

The SAFECOM SoR provides needed direction and dimension to the interoperability challenge. It also gives both government and industry access to the leverage mentioned in the second of our recommendations. Industry directly benefits from the SoR architectural perspective because it allows us to align critical research and development efforts with interoperability demand. Public safety and other first responder organizations benefit from the establishment of a standards baseline upon which they can base their sourcing and selection decisions. Certainly, these are again, all good things—but the real measure of success will be in the integration and deployment of new capabilities directly addressing both new threats of terrorism and old threats like natural disasters.

The new application horizons that interoperability offers are critical components in ensuring the safety and security of our country. The ability to provide integrated command and control across multiple responders with different technology baselines, or the ability to first locate and then dispatch critical materials and resources to specific locations, will make huge differences in our ability to respond to potentially disastrous events. These applications come from many sources, not the least of which, is the DoD and aggressive reuse of technologies developed to support our troops in foreign operational theatres should be accelerated, wherever appropriate, because the investment is R&D has already been made. This is not suggest, however, that DoD technologies are immediately applicable. Public safety and first responder environments are not the same as a foreign operational theatre and solutions need to be carefully vetted to ensure that their use (as well as any unintended consequences of their use) meet our laws and fit the business and operational needs of the user community. For example, systems requiring fixed infrastructures that incur high sustainment costs are not likely to be economically viable for internal US deployment.

Mr. REICHERT. Thank you, sir. Thank the witnesses for their testimony and I have a couple of questions and we will move to the other members.

We heard on both panels some common themes, and I think that Mr. Gass, is that how I would pronounce it correctly, kind of summed it up for me in the five points that he made with national security frequency spectrum, lack of standards, common operating structure would be, if I understood that correctly, would be incident command sort of a structure, and then the phaseout of the legacy systems, which some of the other witnesses have testified to.

I understand there is no silver bullet and all of these five are in process and have been for years, but I asked the last panel, the first panel this question, and I want to pose it to the members of this panel. Is there any one thing that we can commit to right now today that needs to be done that is foremost in your minds, or all five of these equally have to be pursued right now? Is there something today you would jump on if you were given direction?

Mr. MORGAN. If I may, Mr. Chairman, I think that the number one recommendation that I would make to you is to recognize, and certainly NIJ recognizes, in the U.S. we have 19,000 law enforcement agencies, 4,500 correctional agencies, several hundred crime labs, innumerable social agencies which are part of this picture, and that doesn't include public safety and the commercial sector that would be involved. So you have an enormously complex policy

environment in which to solve the interoperability problem. And so, the first thing to do is take a deep breath and realize it is going to be a long-term problem to put in the basic foundations in terms of standards and policies necessary to provide for interoperability to be in public safety, not next year, not in 5 years, but over the long haul. And if you take a long-term view and you execute policies that reflect that, I think you will be very successful in the long-term.

Mr. REICHERT. Anyone else?

Mr. BOYD. I would like to suggest that probably the most important thing you can do is exactly what this committee has been doing now I think for the last 2 or 3 years. I first got involved in interoperability when we were supporting PSWAC back in 1993. At that time there was an occasional member, might be occasional article, staffer who would ask questions about interoperability.

The intensity of interest on the part of this committee isn't just remarkable, I think it is incredibly important to the public safety community. I frankly think that is the most important first step, and I would ask you not to stop.

Mr. REICHERT. Well, I might just take a moment to comment on that. We aren't going to stop. When we started this process several months ago we made a commitment to the people in our first hearing that we were going to help to solve this problem, and a lot of it I think stems from all the hard work that was done before I got here and certainly my personal interest in those who wear the badge. Firefighters and first responders and police officers across this Nation I have a close relationship with, as you well know. So we will continue our fight and help you in any way that we can.

I have just noticed now, out of law enforcement and a Member of Congress, that sometimes things move quite a bit slower and need to be nudged quite a bit. So if you hear a little bit of urgency in our questions and a tone of impatience, I know that you will understand that because it does, as Ranking Member Pascrell has mentioned earlier, we are talking about lives here. Just think about that for a moment. It has been going on for years. That is how important this is.

I think that, Mr. Gass, you really have captured in your testimony some very important thoughts. And I am interested, as you said, you are outside the Beltway and have a different perspective. Having listened to the two panels and their testimony, do you have a better sense really that there is a promising federally coordinated effort in putting together all the five critical aspects that you have described for us in your testimony?

Mr. GASS. Yes, sir. I believe they are going in the right direction. I wish some of it had started sooner and was further along. All indications are that the brethren have gotten together and they have come to these conclusions and most of the Federal agencies are acting in accordance, having heard those issues from the responders, and trying to go in the right direction.

I was familiar with—was on the Standards Coordinating Committee of the IAB and my interest was on personal protective clothing and equipment standards, specifically respirators. It became painfully obvious to me just coming into this business just how cumbersome is the standards development process, especially if you

have to go through the formal rule making process. Thankfully, NIOSH short cutted that and did it by policy and we got there in a couple of years instead of 5 or 6 years.

But this whole standards development process maybe takes longer than it should. That is just perhaps my observation. I think we are well along that way but I do also think the important thing is that at the end of it, whatever standards we have also calls for testing and certification. I think we do a disservice if we allow the manufacturers to self-test and say we are good. We need to assure the response to the community that what they are bringing to the table is what they say it is.

Mr. REICHERT. I agree.

Mr. Pascrell.

Mr. PASCRELL. Mr. Chairman.

Mr. Morgan, to what extent does the NIJ comply with the Homeland Security Act mandating use of voluntary consensus standards?

Mr. MORGAN. As you may know, Mr. Pascrell, NIJ actually has authority under the Homeland Security Act to promulgate standards for law enforcement and other criminal justice agencies, and our most notable standard in that case is the body armor standard, and we are very proud of it. We have had our 3,000th save of a law enforcement officer from body armor. So NIJ is very, very committed to standards development across the law enforcement arena and has for many years contributed to the support of the P25 effort and other standards development efforts within the communications area.

We also coordinate very, very closely with both SAFECOM and NIST in all of our technology and research development efforts, and I can say that we are very, very impressed and would like to congratulate the work that NIST is doing not only in the standard development process but also the critical component, which is the compliance assurance process which is necessary, we have found, in other law enforcement equipment areas to ensure that the standards aren't a hollow shell.

Without compliance testing you don't know whether those manufacturer claims of compliance are true or not. So NIJ very much supports those kinds of activities and incorporates it in all of our 17 different investment areas for technology, research and development for criminal justice.

Mr. PASCRELL. How does, for instance, the National Institute of Justice hold vendors accountable?

Mr. MORGAN. The primary way that we have to hold them accountable is through the standards and compliance assurance process. We are obviously, even within the Federal picture for criminal justice, a fairly small player. We don't even necessarily have nearly the money of a Bureau of Justice Assistance to purchase equipment and things of that nature. We do have that hook of whether a particular piece of equipment meets the particular NIJ standard in an area. So, for example, going back to body armor, the Bullet Proof Vest Partnership program requires NIJ compliance for all body armor that is purchased with Federal funds. The NIJ standard has been successful in that area because the vast majority of State and local governments will call that out in their procurements.

They have learned through hard experience over many, many years that not having NIJ compliance for their body armor is a real problem from a quality assurance perspective in keeping the officers safe. I think that the public safety community is going to see over the next few years the importance of that same philosophy with respect to purchasing communications equipment, they see the compliance assurance programs and standards development programs of NIST under P25 and other standards mature.

Mr. PASCRELL. Thank you very much.

Mr. Orr, the National Institute of Standards and Technology, do you think that the labs that you have to work in order to assess the technology are adequate, are they updated constantly, are they outdated?

Mr. ORR. I think the labs that we have are certainly adequate. I think we have a world class laboratory environment in NIST both in Gaithersburg, Maryland, and out in Boulder, Colorado. The work that was originally done over the last, say, 3 years to determine the issues regarding the P25 standards and its implementation and the P25 subscriber units, what that taught us is that, one, obviously there needs to be some kind of objective testing of the products.

The second thing it taught us is, we do not have enough money to do that testing nor do we have enough staff to test all the various products that are available. So the compliance assessment program that we are currently working on in partnership with the public safety community's association leadership that is involved in P25, as well as industry, is going to have industry and the manufacturers pay for testing of that equipment in certified accredited laboratories.

So in the future the tests will not be done at NIST. The tests will be done at accredited laboratories paid for by the manufacturers themselves.

Mr. PASCRELL. Thank you. I am glad you pointed that out. It is very important, I think.

Mr. Gass, according to your testimony there is a lack of leadership, and that is the main reason why the Nation has not progressed in using the technology available to improve interoperable communication.

What Federal incentives would you propose to move State and local jurisdictions in the direction of standard compliance, standards compliance?

Mr. GASS. I believe that once we have those standards out there and a means to test and certify them, when the local jurisdictions make their decisions on equipment to purchase, they will go in that direction whether we are talking Federal dollars or their local dollars. We do not have that now, so they will buy their communications equipment based on their local jurisdictional needs and resources and budgets. But once we begin to shape in this vision and have a set of standards, I think they will fall in line and want to go that way. And then all we have to worry about is, Okay, how do we transition from here and now to the objective state?

Mr. PASCRELL. Thank you.

I have one final question if I may, Mr. Chair.

Mr. Walker, your testimony calls for an increased private-sector role; you want to improve that role, you want to increase that role with regard to securing critical communication infrastructure.

There have been many instances when private industry has been hesitant to detail their plans because of propriety issues. How are we going to adjust that?

Mr. WALKER. I think it is a critical issue, but at the same point in time, the infrastructure that we are responsible for operating as a part of our businesses is managed and provides a security cordon of our own that is necessary for the insurance that we can continue that business. They are the first line of defense if there is an attack on those facilities.

Public safety responds primarily to the people that are there who are already in a security mode, and not having those people connected to those same kinds of public safety systems means that the response coordination is delayed until public safety actually arrives at the location.

When you look at port facilities or some of the other truck transfer facilities that we as an industry are responsible for managing and maintaining, the availability and the responsiveness of those private security forces is a key component of the way we can defend and detect.

So, yes, there is a propriety issue and, yes, there is probably an issue with respect to the way the law is actually applied to those private security forces in the commission of their own responsibilities; but having access from an interoperability perspective is something we think is an important goal.

Mr. PASCRELL. Thank you, Mr. Chairman.

Mr. REICHERT. Again, just a follow-up question or two just to come at this issue just a little bit differently. This panel is saying clearly that technology is not the problem; technology exists to solve the interoperability problem. Is that a correct statement? Yes.

So what is the problem? I came at you before. What do we need to do? What is the problem? We have technology out there.

I know we have already rehashed some of this. Is it leadership within the Federal Government that you are looking for?

Mr. BOYD. I think clearly that is part of it. Part of what we are trying to do is work with States to help them understand how to do this so that they can build statewide plans that are really supported from the ground up.

One of challenges, I think, at the Federal level is that we sometimes think that we can push a solution down. What we need to do is pull a solution up. We need to have them design it at the bottom level.

Your department, your sheriffs department, for example, had its own mission and its own citizens and its own requirements to meet. We need to figure out how we protect that mission and at the same time provide both incentives—and sometimes those incentives just amount to helping people understand why they are useful to them to begin to cooperate with adjacent jurisdictions. In fact, some places have done that really well already; some have not.

Mr. Walker, I think, really hit the nail on the head. The toughest of all the nuts to crack, but the most important, is governance because that requires leadership at the local agency and political

level; and it requires commitment to agree, a commitment to work together.

Mr. REICHERT. I can identify with that problem very personally. To get people to work together, 38 police departments within King County and the turf wars that might cause is a huge problem to overcome. I understand that.

Dr. MORGAN.

Mr. MORGAN. It is absolutely true that technology is not the problem. Technology does exist today that if the United States were a unitary place without thousands and thousands of jurisdictions you could deploy systems that were interoperable, there is no question.

However, I just want to add one thing about that, and that is, technology development, research and development, can play a contributing role to solutions in certain locations and certain ways that can be helpful. It is a multifaceted problem; you will have multifaceted solutions. And every solution, because all the problems have grown up from unique situations in the State and local arenas where they exist today, you are going to need a variety of different kinds of technology solutions to be able to make interoperability happen over the long haul.

Mr. REICHERT. Thank you.

Just one quick question. So working with the State government officials and local police departments and counties and sheriffs departments, sheriffs offices, you also have to work with yourself, so you have NIST and the Federal Government and NIJ and SAFECOM.

Do NIST and NIJ and SAFECOM meet? Do you all meet? How often do you all meet? You have a meeting right after this hearing, right?

Mr. ORR. At a bar. I meet up with the members of SAFECOM, NIJ. We attend each others' program meetings that occur usually quarterly. We see each other at various open standards meetings that we go to. I show up downtown and meet with the staff of these offices probably once a week.

But NIJ and SAFECOM come to our program reviews. I go to SAFECOM's and NIJ's, and SAFECOM goes to NIJ's and ours. So we are very coordinated and, in fact, share a lot of resources.

My staff helps peer review of NIJ's programs and SAFECOM's. We get funding from SAFECOM; we get funding from NIJ. There is a lot of coordination and a lot of cooperation from them.

Mr. REICHERT. Mr. Pascrell, any additional questions?

I thank the witnesses for their valuable testimony and the members for their questions. The members of the committee may have some additional questions for the witnesses and we will ask that you respond to these in writing. The hearing record will be open for 10 days.

Mr. REICHERT. Without objection, the committee stands adjourned.

[Whereupon, at 4:20 p.m., the subcommittee was adjourned.]

○