2007

OIC Industry Roundtable Report

May 9-10, 2007
Washington, DC

Hosted by the Science & Technology Directorate's Office for Interoperability and Compatibility within the Department of Homeland Security

Letter from Dr. David Boyd, Director, Command, Control and Interoperability

Law enforcement, fire response, and emergency medical services responders rely on communications technology to support them in dangerous and frequently changing environments. Responders often cannot talk to some parts of their own agencies—let alone across cities, counties, and states. Emergency responders—police officers, fire personnel, emergency medical services (EMS)—need to share vital voice and data information across disciplines and jurisdictions to successfully respond to day-to-day incidents and large-scale emergencies. Many people assume that emergency response agencies across the Nation are already interoperable.

In fact, emergency responders often cannot talk to some parts of their own agencies—let alone communicate to agencies in neighboring cities, counties, or states. Too often, inadequate and unreliable communications compromise emergency responders' ability to respond effectively to incidents that range from day-to-day operations to large-scale emergencies. Ineffective communications risk the lives of responders in the field, and can mean the difference between life and death for those awaiting help.

The 2007 Office of Interoperability and Compatibility (OIC) Industry Roundtable brought together members of the emergency response community, the communications industry, and government officials to collaborate on key issues inhibiting establishment of interoperable communications systems for the emergency response community. Over the course of the two-day event, participants chose from a variety of roundtable discussions that addressed critical aspects of the interoperability challenge from multiple stakeholder perspectives. The object of these discussions was the establishment of public-private partnerships as well as recommendations for next steps that can advance communications interoperability.

Interoperability is not solely a technology problem that can be solved with the "right" equipment or the "right" communications system. Interoperability is a complex, multi-dimensional issue. There are no "silver bullet" solutions. Some technology solutions are useful for command elements, but are impractical for individual emergency responders. Achieving interoperability involves tactical, technological, strategic, and cultural changes.

As we look to the future, we need to remind ourselves that it is only through partnerships that we can truly achieve interoperability for the Nation. Put another way, Washington can't do it all. State and local governments must continue to take constructive steps towards building a better system. We look to you—our committed industry partners—to help us succeed in our mission to detect, protect against, and recover from major incidents. This Industry Roundtable represents a significant step toward aligning technology solutions with the needs of emergency responders on the frontlines. Events like this Industry Roundtable bring together the right people—industry representatives, emergency responders, and government officials—to collaboratively address critical interoperability issues. We thank you for your participation in this event and your continued dedication to this critical, national mission.

Table of Contents

Industry Roundtable Agenda

Wednesday, May 9, 2007	
7:30 - 8:30	**Registration Check-in and Continental Breakfast**
8:30 - 9:35	**Office for Interoperability and Compatibility (OIC) Welcome** **Dr. David Boyd,** Director, Command, Control and Interoperability, DHS **Office of Emergency Communications (OEC) Welcome** **Col. Victoria Velez,** Director, Office of Emergency Communications, DHS **DHS Science & Technology Directorate Welcome & Opening Remarks** **Under Secretary Jay Cohen,** Under Secretary, Science & Technology Directorate, DHS **Q & A with Under Secretary Cohen, Col. Velez, & Dr. Boyd**
9:35 - 9:50	**Break**
9:50 - 10:30	**OIC Vision & Strategy** **Dr. David Boyd,** Director, Command, Control and Interoperability, DHS
10:30 - 12:00	**"A View from the Front: The Emergency Response Experience"** **Chief Brian Fennessy,** Battalion Chief and Director of Air Operations, San Diego Fire-Rescue Department **Chief Eric Mello,** Chief, Westerly Police Department **(Ret) LTC Michael Todorovich,** Interoperable Communications Coordinator, West Virginia Department of Military Affairs and Public Safety
12:00 - 1:45	**Lunch with Keynote Speakers** **Secretary Michael Chertoff,** Secretary, Department of Homeland Security **Representative Dave Reichert,** Member, Committee on Homeland Security, US House of Representatives
2:00 - 3:30	**Breakout Series I:** **Session A: "Grant Guidance: What You Need to Know"** **Tony Frater,** Deputy Director, Office for Interoperability and Compatibility, DHS **Scott Kelberg,** Director, Technical Assistance Division, Capabilities Division, Federal Emergency Management Agency, DHS **Laura Pettus,** National Telecommunications and Information Administration, US Department of Commerce **Session B: "Emergency Interoperable Data and Messaging Standards Efforts"** **Mike Daconta,** Vice President, Enterprise Data Management, Oberon Associates, Inc. **Theresa Lynn Hadden,** Information Architect, Fairfax County, Virginia **Chip Hines,** Program Manager, Disaster Management e-Gov Initiative, DHS **Elysa Jones,** Engineering Program Manager, Warning Systems, Inc **Donna Roy,** Director, Enterprise Data Management Office, Office of the CIO, DHS **Paul Wormeli,** Executive Director, IJIS Institute
3:30 - 3:40	**Break**
3:40 - 4:20	**Full Plenary: Report out from Breakout Series I**
4:20 - 4:30	**Day One Closing Thoughts, Plans for Day Two**
4:30	**Adjourn for Day & Optional K9 Demo from the Westerly Police Department**

Thursday, May 10, 2007	
7:30 - 8:30	**Continental Breakfast**
8:30 - 8:45	**Day Two Welcome, Agenda Review, Quick Recap of Day One**
8:45 - 9:00	**Break**
9:00 - 10:30	**Breakout Series II:** **Session A: "P25/CAP: What Does It All Mean?"** **Eric Nelson,** Electronics Engineer & Team Leader of the Interoperability Research Laboratory, Institute for Telecommunication Sciences (ITS) **Dereck Orr,** Program Manager, Public Safety Communications System, National Institute of Standards and Technology (NIST) **Session B: "VoIP: What It Can Be"** **DJ Atkinson,** Lead Electronics Engineer, National Telecommunications and Information Administration (NTIA), Institute for Telecommunication Sciences (ITS) **Linda Fuchs,** Program Manager, Department of Management Services, Enterprise Information Technology Services, State of Florida **Luke Klein-Berndt,** Chief Technical Officer, Office for Interoperability and Compatibility, DHS **Captain Robert Kuzma,** Technology Implementation and Risk Assessment, San Francisco Fire Department
10:30 - 10:45	**Break**
10:45 - 11:30	**Full Plenary: Report out from Breakout Series II**
11:30 - 12:00	**Keynote Speaker** **Representative Bennie G. Thompson,** Chairman, Committee on Homeland Security, US House of Representatives
12:00 - 1:00	**Lunch with Keynote Speaker** **Assistant Secretary Greg Garcia,** Assistant Secretary for Cyber Security and Communications, Department of Homeland Security
1:15 - 2:45	**Breakout Series III:** **Session A: "National Interoperability Baseline Study: So What?"** **Troy Cribb,** Majority Counsel, Senate Committee on Homeland Security and Governmental Affairs **Tony Frater,** Deputy Director, Office for Interoperability and Compatibility, DHS **Veronique Pluviose-Fenton,** Majority Senior Counsel, House Committee on Homeland Security **Colonel Victoria Velez,** Director, Office of Emergency Communications, DHS **Marilyn Ward,** Executive Director, National Public Safety Telecommunications Council (NPSTC) **Session B: "Public Safety Broadband: Can It Really Work?"** **Dr. David Boyd,** Director, Command, Control and Interoperability, DHS **Christopher Guttman-McCabe,** Vice President, Regulatory Affairs, CTIA - The Wireless Association **Gregory Henderson,** Manager of Broadband Technology, Tyco Electronics Wireless Systems Segment **Robert LeGrande II,** Interim Chief Technology Officer, Washington, DC Office of the Chief Technology Officer (OCTO) **Harlin McEwen,** Chairman, Communications and Technology Committee of the International Association of Chiefs of Police (IACP) **Morgan O'Brien,** Co-founder and Chairman, Cyren Call Communications **John Powell,** Chair, Interoperability Committee and Software Defined Radio Working Group of National Public Safety Telecommunications Council (NPSTC)

2:45 - 3:00	**Break**
3:00 - 3:45	**Full Plenary: Report out from Breakout Series III**
3:45 - 4:00	**Closing Thoughts, Next Steps**
4:00	**Adjourn**

Welcomes and Opening Remarks

Dr. David Boyd, Director, Command, Control and Interoperability, and the Director of the Department of Homeland Security's (DHS) Office for Interoperability and Compatibility (OIC), welcomed participants and described the purpose of the day. He was followed by Colonel Victoria Velez, Director of the Office of Emergency Communications (OEC) at DHS, and Jay Cohen, Under Secretary for Science and Technology (S&T) at DHS.

From left: Under Secretary Jay Cohen, Colonel Victoria Velez, Dr. David Boyd

Dr. David Boyd

Director of the Department of Homeland Security's Office for Interoperability and Compatibility (OIC)

- Over the past four years OIC has brought together key stakeholders and emergency responders from the field to identify and discuss the most significant and necessary initiatives to improve interoperable communications.

- We are committed to strengthening interoperable communications through our comprehensive, "system of systems" approach—one that is driven from the bottom up.

- OIC's many successes are due in large part to this philosophy—we know that the development of a successful solution to improving emergency response communications interoperability requires a focus on user needs and requirements.

- Last March, we brought together many of you—emergency responders, policy makers, and industry professionals—at our Inaugural Industry Summit to collaborate on the challenges facing interoperability and the technological possibilities available to overcome these challenges.

    - This event initiated a critical conversation on interoperability initiatives between industry and the emergency response community. It also provided industry professionals with an opportunity to offer feedback and thoughts directly to the emergency response community and Federal leadership.

- We will spend the next two days discussing strategies and solutions that advance the emergency response community.

    - We will discuss your identified topics of interest: Grant Guidance; Project 25/Compliance Assessment Program; Voice over Internet Protocol (VoIP);

emergency response data messaging standards; broadband; and the findings and future of the National Interoperability Baseline Survey.

- Your thoughts and suggestions as you move through the discussions and breakout sessions are critical to the success of this Roundtable.

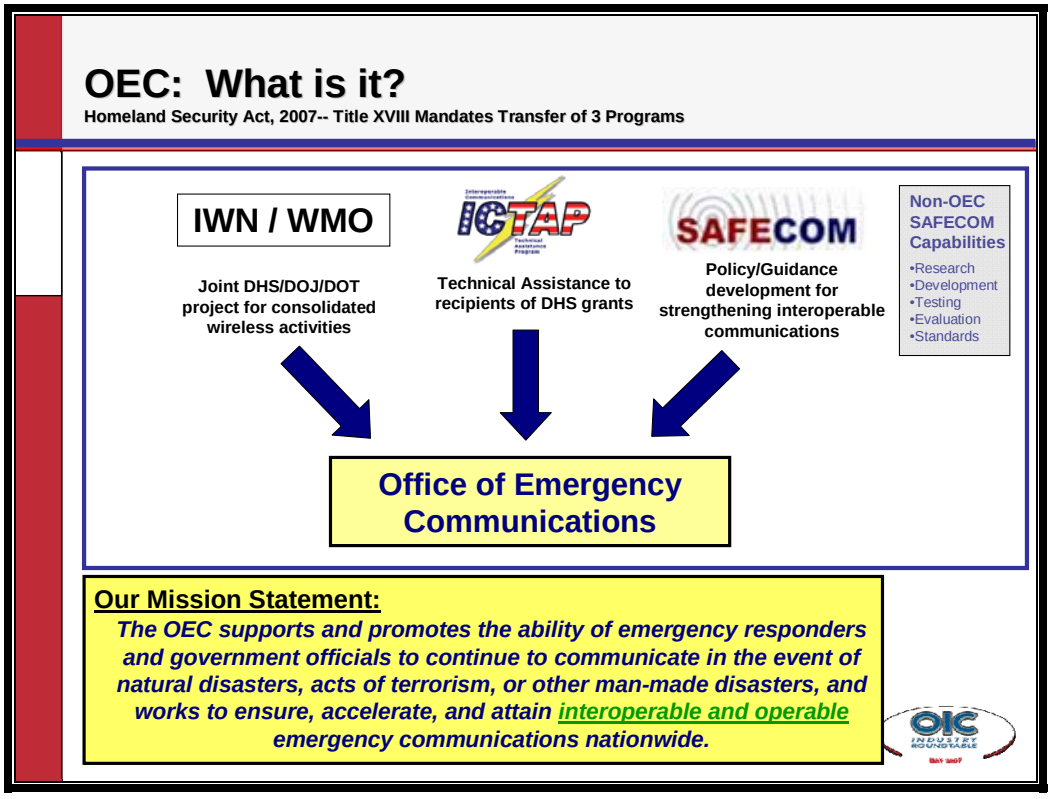
Colonel Victoria A. Velez
Director of the Office of Emergency Communications (OEC), DHS

- The Department of Homeland Security Appropriations Act, 2007 gave the OEC the responsibility to administer certain elements of the SAFECOM program.
    - SAFECOM's authorities related to research, development, testing & evaluation, and standards will remain in the OIC within the S&T Directorate.

- Three organizations were transferred to OEC:
    - Wireless Management Office (WMO)
    - Interoperable Communications Technical Assistance Program (ICTAP)
    - Parts of SAFECOM—outreach, standard operating procedures (SOPs), procedures, tools.

- OEC is in the Directorate for National Protection and Programs.

- OEC is starting to support the Public Safety Interoperable Communications (PSIC) grant process, and will evaluate the state plans (will provide feedback if plans are submitted before November 1).



Some OEC Roles and Responsibilities

- Establish capabilities supporting seamless, interoperable communications across government at all levels.

- Administer SAFECOM, ICTAP, and Integrated Wireless Network (IWN).

- Conduct outreach and foster development of interoperable emergency communications capabilities by local, tribal, state governments.

- Provide technical assistance (TA) in the use of interoperable emergency communications to local, tribal, state governments.

- Promote SOPs, best practices, and tools for interoperable emergency communications capabilities relating to incident response.

- Support the Executive Branch as required.

Some OEC Priorities

- Conduct National Baseline Assessment.
    - Two-phased approach

- Prepare for hurricane season and other events.
    - With NCS and FEMA

- Develop a National Emergency Communication Plan.

- Continue to build and solidify partnerships with stakeholders.

Under Secretary Jay Cohen

Under Secretary for Science and Technology (S&T)

- The S&T Directorate is committed to serving our customers, the components that comprise the DHS—and *their* customers—the hardworking men and women on the front lines of homeland security, especially emergency responders. They need ready access to technology and information to perform their jobs more efficiently and safely.

- Accelerating the delivery of enhanced technological capabilities to meet the requirements of S&T's customers, and fill key capability gaps in homeland security, is one of the three goals identified for the S&T Directorate.

- A priority for me personally and for DHS on the whole is the strengthening of interoperable communications—the seamless transfer of incident-related information though both voice and data.

- Integral to achieving this goal are fully adopted and deployed voice and data standards *and* engaged emergency response leadership contributing to governing bodies that implement and spur organizations to interoperability.

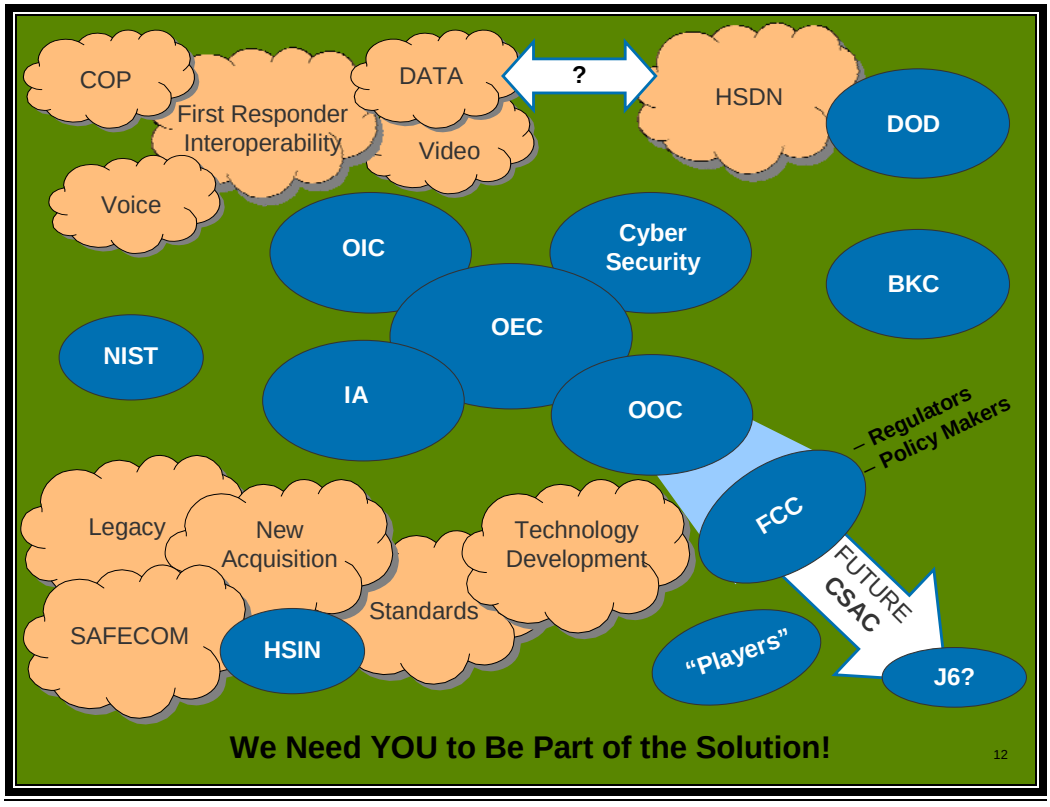
- Our national strategy for improving interoperability must take into account *all* of the factors critical for a successful interoperability solution—governance, SOPs, training and exercises, usage, *and* technology.

- Industry is a valued partner of S&T, and we need your continued participation in developing solutions for homeland security applications vital to our effort to safeguard the Nation.

- As part of our outreach efforts to encourage greater industry participation, the Directorate will join The National Defense Industrial Association (NDIA) in hosting our first S&T Stakeholders Conference on May 21-24.

    - The conference will inform government, industry, and academia of the direction, emphasis, and scope of the research investments by the Directorate, and provide information about business opportunities.

    - The conference will present the Directorate's new organization, explain how to do business with the S&T research enterprise, and provide visibility into new and emerging technologies through an Innovation Gateway Marketplace.



Q&A

Q Is DHS going to do something about the potential for interoperability conflicts (e.g., interference)? New Jersey requires a radio repeater. Has anything come out from OIC or OEC to require such identifiers from the vendors?

A This is a difficult problem, but progress has been made. OEC's new frequency guide, and the statewide planning process, will help improve coordination.

Q How is OEC going to provide the same comprehensive practitioner/emergency response input that OIC has been doing?

A The SAFECOM Executive Committee (EC) is a wonderful vehicle for sharing information. OEC wants to continue the process. It is included in Col. Velez's budget.

Q How will the Under Secretary's FY08 budget support his priorities?

A We're increasing the number of investment vehicles like the quick-turnaround Homeland Innovative Prototypical Solutions (HIPS) and High Impact Technology Solutions (HITS) projects—expected to receive $60 million in FY2008—as well as Broad Agency Announcements (BAAs). As systems like BioWatch 2 transition to the customers, and spending for them decreases, even more money will be made available, and will allow us to invest in new or successor projects, like BioWatch 3.

Q We have a proven product and we want to get into the public safety market. Where should we start? What office do we work through to get our product known?

A For DHS, you may want to contact the Wireless Management Office or some of the component agencies like the Coast Guard, or Borders/Maritime. Most of your customers though will be states and localities, so your challenge is to generate their interest, and perhaps have them apply for grants in order to fund the purchase. Ensuring that your equipment is on the Authorized Equipment List and meets applicable standards is also recommended.

OIC Vision and Strategy

Dr. David Boyd

Office for Interoperability and Compatibility

- The OIC is working with the emergency response community and Federal partners to address the multiple dimensions of interoperability to improve local, tribal, state, and Federal emergency preparedness and response.

Vision

- Interoperable communications is an attainable, albeit ambitious, goal.
- The emergency response community has worked with OIC to articulate a vision for interoperability.
- Emergency responders operating with seamless interoperability will be able to respond to an incident anywhere in the Nation, using their own equipment, on any communications system, and on dedicated public safety spectrum as needed and authorized.
- This eventual goal will not happen overnight. To achieve interoperable communications solutions, the emergency response community, industry, and the Federal Government must work together using a common approach.

Strategy

- Ultimately, achieving interoperability involves a technological, strategic, tactical, and cultural change. A national strategy for improving interoperability must take into account all of the factors critical for a successful interoperability solution—governance, SOPs, technology, training and exercises, and usage.
- The development of a successful solution to improve interoperable communications requires a focus on user needs and requirements. The input of both practitioners and policy makers, across disciplines, jurisdictions, and levels of government, who are able to represent their own needs and to strategically approach the greater needs of the emergency response community, must be included in any solution.

- Any strategy for improving emergency response interoperable communications must be based on user needs and driven from the bottom up.

- Because local jurisdictions own, operate, and maintain the majority of the Nation's communications infrastructure, it is critical that interoperability solutions be practitioner-driven; any solution should come from the community that is best able to own and implement the solution.

Challenges

- **Cultural Challenges**: Cultural challenges jeopardize interoperability progress.
  - Limited and fragmented planning, accompanied by a lack of coordination and cooperation, is commonplace across local, state, and Federal agencies and across government levels.

- **Technological Challenges**: Although technology is an important element of interoperability progress, it is not the sole driver of the solution.
  - Success in conquering cultural and financial issues is essential and should drive technology procurement.
  - Technology is highly dependent upon existing infrastructure within a region. Multiple technology solutions may be required to support interoperability.

- **Financial Challenges**: Solving the interoperable communications problems is expensive.
  - Traditionally, emergency response agencies would develop their own communications systems and only consider the need to communicate internally.
  - Today, more jurisdictions are working to strengthen their interoperable communications. However, there is limited funding for emergency response agencies and increased competition for those resources.

OIC Approach to Challenges

- OIC, in partnership with the emergency response community, is creating the capacity for increased levels of interoperability by developing tools, best practices, and methodologies that practitioners can put into effect immediately.

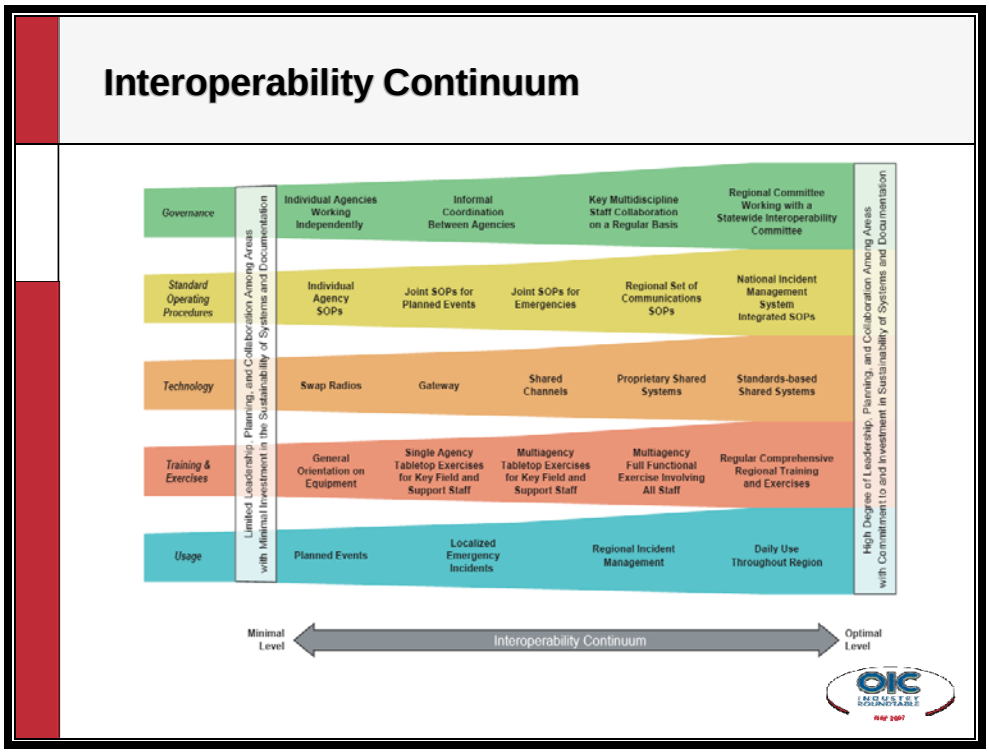
- OIC is also improving incident response and recovery by developing tools and messaging standards that help emergency responders manage incidents and exchange information in real time.

- OIC is committed to developing high-quality tools and resources to help the emergency response community migrate towards an interoperable "system of systems" nationwide.

- OIC resources capture best practices and lessons learned from the field, practitioner-driven requirements, and input from emergency responders nationwide.

- OIC developed the Interoperability Continuum to help the emergency response community and policy makers plan and apply interoperability solutions.

- The tool identifies five critical success factors that must be addressed to develop a sophisticated interoperability solution: governance, SOPs, technology, training and exercises, and usage of interoperable systems.
- The degree of interoperability depends upon the improvement of all five of these elements—no one factor (e.g., technology) is the solution to achieving interoperability.
- Jurisdictions across the Nation are using the Continuum to track progress in strengthening interoperable communications.



- OIC also worked with practitioners to develop the Statement of Requirements (SoR), a comprehensive set of requirements enabling manufacturers to design equipment that meets emergency responders' communications needs.
  - The SoR defines the basic functional and operational requirements for emergency response communications.

- OIC has developed a wide spectrum of tools and resources designed to strengthen voice and data interoperability. All of these tools can be found at www.safecomprogram.gov.

Standards and VoIP

- The acceleration of standards also is a key component of OIC's approach to strengthening voice and data interoperability.
  - OIC supports the acceleration of Project 25 (P25) standards that help produce equipment that is interoperable and compatible regardless of manufacturer. P25 is a suite of eight standards intended to help produce equipment with such characteristics.

- At the request of Congress, OIC is working with the National Institute of Standards and Technology (NIST), the Department of Justice, and the P25 Steering Committee to develop and implement a Compliance Assessment Program, or CAP.
- CAP will validate that P25-standardized systems are indeed P25-compliant, and that equipment from different manufacturers can interoperate. This effort will help ensure the appropriate use of Federal grant dollars.
- Disaster Management (DM) leads the Information Exchange Standards Initiative, a public-private partnership to create messaging standards to share information between disparate incident management systems and software applications.
- On August 22, 2006, the NIST Office of Law Enforcement Standards, in conjunction with OIC, brought industry professionals together with members of the emergency response community to discuss the role of Voice over Internet Protocol in emergency response communications.
    - Among other conclusions, the emergency responders agreed that there is a need for VoIP standards—interoperability to the lowest common denominator must be maintained.

The Road Ahead

- We're making progress. OIC's National Interoperability Baseline Survey indicated that approximately two-thirds of emergency response agencies use interoperable communications.
    - In May-July 2006, DHS surveyed approximately 22,400 randomly selected law enforcement, fire response, and EMS agencies nationwide.
- Though many challenges remain, the Federal Government is committed to ensuring that the Nation's emergency response community has the necessary tools and resources to ensure communications systems are interoperable when they have to be.
- Both the emergency response community 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. This Industry Roundtable represents a step in this direction.

A View from the Front: The Emergency Response Experience

Session Synopsis

View from the Front: The Emergency Response Experience session was designed to remind members of industry and the Capitol Hill and public safety communities why the Federal Government continues to work on interoperability issues. Three representatives from the emergency response community presented real-life examples of critical incidents that highlight the benefits and challenges of technological advances in emergency response communications.

Panelists

The panelists included leaders from the emergency responder community:

- **Chief Brian Fennessy,** *Battalion Chief and Director of Air Operations, San Diego Fire-Rescue Department*
- **Chief Eric Mello,** *Chief, Westerly Police Department*
- **LTC (Ret.) Michael Todorovich,** *Interoperable Communications Coordinator, West Virginia Department of Military Affairs & Public Safety*

Session Key Points

- The challenge of interoperability is a critical daily struggle in the emergency response community.
- There is an immediate need for continued improvement of interoperability for legacy technologies and swifter progress with interoperable communication tools for emergency responders in emerging venues such as VoIP and broadband.

Chief Brian Fennessy, *Battalion Chief and Director of Air Operations, San Diego Fire-Rescue Department*

- In 2003, a significant wildfire broke out whose flames spanned over 75 million acres in only 14 days. At the time San Diego operated off a trunked 800 MHz system. Surrounding areas did not have this capability, and state and Federal organizations were on VHF. The wildfire burned over 12,000 acres per hour and massive fatalities occurred as people left their homes. The whole system had collapsed. The after-action report indicated that everyone was acting independently through their own systems. All information was sent through an ineffective choke point.
- We need equipment that is reliable, cost-effective, and easy to use.
- Industry needs to:
  - Collaborate with practitioners in the development of technology.
  - Move to open standards.
  - Review the SAFECOM initiatives and approaches to make sure their products are consistent.
- Our successes include a Regional Command Control Project that includes the City of San Diego, San Diego County, and the California Department of Forestry and Fire Protection. Our system allows for the transmission of voice, data, and video in real-time. We also have a Tactical Interoperable Communications Plan (TICP) in place, as well as Interagency Air Operations that enable air tankers and helicopters to communicate with each other.

- From a funding perspective, we are struggling to sustain systems after initial grant funding.

Chief Eric Mello, *Chief, Westerly Police Department*

- Although our district is a small town in a small state, we get over 35,000 calls per year. We are surrounded by smaller agencies and we rely on each other. We all operate under different chiefs and different protocols, which inevitably create challenges. Despite our small size, we have the same types of complex needs as large cities with large budgets.
- Industry tends to address large-scale emergencies. Although these are very important, the emergency response community faces challenges everyday on a smaller scale that require interoperable technology.
  - When the emergency response community was notified that there was a bomb on a train, the six police agencies and seven fire agencies that arrived on the scene relied on cell phones for dispatch. We were otherwise unable to communicate with each other.
  - An incident due to a toxic chemical spill occurred in a grocery store. Six different EMS responder groups, the FBI, and multiple Environmental Action Teams arrived on the scene. This convergence created a great need for interoperability, even though this wouldn't be classified as a large-scale event.
- As a chief of a small agency I am painfully aware of the constraints of funding. Maintenance costs are now in the thousands of dollars. Volunteer fire agencies cannot move beyond high frequency band due to costs.
- Moving to an 800MHz system two years ago created additional challenges: now our police agency cannot connect with neighboring agencies that are still on the high band system.

LTC (Ret.) Michael Todorovich, *Interoperable Communications Coordinator, West Virginia Department of Military Affairs & Public Safety*

- During a fire incident in Upshire County, WV, families were told that their loved ones were alive when they were not. The lack of interoperable systems created that kind of communication breakdown.
- Mountains prevent communication, and the complex programming of P25 systems make communication more difficult for more rural areas.
- We recommend that Industry:
  - Make the technology simple and easy to use.
  - Deliver when you say you will.
  - Get out of your office and see the real action.
  - Take the National Incident Management System (NIMS) course.

Emergency Response Panel – Q & A

Q Where do you go for information on interoperability?

A *Mello*: I rely on the industry to come to us.

A *Todorovich:* The Internet.

A *Fennessy:* Word of mouth is most effective. If a technology is working, we find out about it. If not, we find out as well. Incidents bring people into the room and that's how we find information.

Q Do communication requests stack up with other budget requests, like Hummers and helicopters? How can you build sustainability?

A *Fennessy:* We are learning the hard way. We haven't always thought about these needs. We've budgeted for these systems, but then they cost more to maintain once the grant funding runs out.

A *Todorovich:* At the state level, the grant procedure has more of an emphasis on budget containment.

A *Mello:* If I lose a high band radio it will cost $500, and if I lose an 800 MHz radio it will cost $2,000. This situation eliminates some agencies because they are afraid of recurring costs.

Q Are you looking at incorporating 911 Call Center architectures into your work with your statewide planning efforts?

A *Todorovich:* We are working towards this. It is important to talk to users to get their needs; otherwise equipment sits on the shelf.

Q I am a part of the Utilities Council and we rely on private internal networks. To what extent have you discussed with your utilities about these same issues of interoperability? What kind of collaboration are you doing with your utilities?

A *Todorovich:* We have included utilities and public access to networks in our interoperability council, our fusion center, and with Amber Alerts. DuPont just bought P25 radios in order to be able to work with us.

A *Fennessy:* We still have a lot to do to incorporate utilities, public access to networks, and even trauma centers. We are moving toward telemedicine that enables us to bring in video access for trauma centers.

Q Where are gateways in your thinking for providing means to interoperate?

A *Mello:* We are just getting into using gateways.

A *Todorovich:* Start with the end state in mind. Gateways are a start. It's all about ultimate functionality.

Q What role do you see with satellite capability?

A *Fennessy:* Costs are too high, but the situation is better than it was. We do use some mobile data computers. We do use satellites in our helicopters and planes. We may explore greater use of this technology.

Keynote Speakers

"It is only through partnerships that we can achieve interoperability for this Nation."
Secretary Michael Chertoff

From Left: Colonel Victoria Velez, Dr. David Boyd, Representative Dave Reichert, and Under Secretary Jay Cohen

Remarks from Secretary Michael Chertoff (Delivered by Under Secretary Jay Cohen)
Secretary, Department of Homeland Security

- It's essential that we improve interoperable communications and it's imperative that this be the responsibility of government at every level, including the Federal level. That's what the 9/11 Commission said, that's what I've been saying since coming to Homeland Security, and that's why it remains one of my main priorities as well as a critical goal for the President and for Congress.

- Now of course we know that interoperability is not a technology challenge alone—one that can be readily solved with the "right" equipment or the "right" communications system. We know that in addition to technology, we have to address critical issues like governance, SOPs, training and exercises, and usage if we want to improve the system.

- Technology remains a fundamental element in addressing interoperability. We have to have technology solutions and we have to make sure that those solutions are aligned with the needs of emergency responders in the field.

- As new technologies are developed—and as policy and protocols that address interoperability are revised—we need to create plans that are flexible and adaptable to an ever-changing environment.

- And if we're going to be flexible and adaptable, the one thing we can't do here in Washington is impose every solution from the top down on the rest of the Nation. What we can and should do is embrace a practitioner-driven approach. At every step in the process—from planning to development, from implementation to testing—we should consult with the grassroots emergency response communities across states and localities: the people and groups who are actually going to use the system.

- At the end of the day, what we want is a framework for a "system of systems." We want emergency responder agencies across this nation to be able to talk to each other during normal, day-to-day operations as well as during large-scale emergencies. Through a national "system of systems," full interoperability can be substantially achieved.

Initiatives and Assessing Our Progress

So what have we done to help strengthen interoperable communications?

- The first thing we've done is devote substantial resources to further this aim. We've provided a total of nearly $3 billion to local and state governments. More funding will be available this year through our Public Safety Interoperable Communications, or PSIC, grant program, which we will co-administer with the Department of Commerce.

- As part of this effort, we've developed coordinated grant guidance to provide consistent criteria for agencies that are purchasing equipment with Federal funds. This guidance helps maximize the efficiency of grant dollars allocated and spent on emergency response communications.
    - It's the first time every communications-related grant agency in the Federal Government has incorporated the same criteria for agencies receiving Federal funds for interoperability.

- The second thing we've done to enhance interoperability is conduct a nationwide assessment to identify the barriers to achieving it.

- Last December, we released the findings of our national baseline survey, the first-ever nationwide assessment of interoperability.
    - The survey looked at five key elements—governance, SOPs, technology, training and exercises, and usage of interoperable communications. It found that roughly two-thirds of emergency response agencies across America use interoperable communications to some degree. Another key finding was that agencies tend to be more advanced in technology than in the other four elements.

- Last year, we also measured the interoperable communications capability in 75 major urban/metropolitan areas. Each of these areas was required to develop a Tactical Interoperable Communications Plan (TICP). Each plan was tested and validated through exercises. Following these exercises, the sites received an after-action report and improvement plan which led to the development of an interoperability scorecard.
    - Each site is now working on improving its weaknesses to ensure it will have interoperability during a major incident.

- The third thing we've done is require states and localities to develop tactical communications plans.
    - This year, we're requiring that each state and territory submit a communications plan by November 1 to ensure eligibility for the PSIC grants.
    - Our goal is to evaluate all the plans through a peer review process by March 31, 2008.
    - By the end of 2008, we'll have released a report verifying whether all 56 states and territories have achieved a minimum baseline of interoperable communications.

- And finally, we've sought to enhance interoperability by helping to accelerate the development of technology standards and requirements. Our goal is to enable states, localities, and their emergency response agencies to know what equipment they need as they plan for interoperability.

- Through our Office for Interoperability and Compatibility, or OIC, in conjunction with NIST, and in partnership with practitioners, the private sector, and other governmental agencies, we've helped ensure that the key components of the P25 technology standards are near completion. Thanks to this partnership, these standards should be completed within the next 18 to 24 months.

- And we're further helping accelerate the development of standards through OIC's Disaster Management, or DM, program. This program supports standards that enable the emergency response community to seamlessly share data across different systems. DM has helped publish four data standards in three years.

- And in line with this acceleration, we're also establishing a Compliance Assessment Program, or CAP, so that equipment from different manufacturers not only functions in an interoperable way, but meets minimal requirements for performance and compliance. The program will ensure that manufacturers who claim their voice communications products comply with published standards actually do comply.

- In addition to accelerating the development of technology standards, we've also developed—with input from practitioners—a Statement of Requirements. This statement defines for the first time the requirements for critical voice and data communications in day-to-day, task force, and mutual aid operations.

- We've also launched the first national effort to help emergency response agencies identify systems gaps and points of interoperability in existing communications systems. We've done this through OIC's publication of two volumes of the Public Safety Architectural Framework, or PSAF.

- Later this year, OIC will conduct projects to test and demonstrate technologies, including data and video, in real-world environments. The pilots will address a host of technologies, including multi-band radios, and will allow OIC to identify the most efficient use of existing dollars to accelerate interoperability across the Nation.

Conclusion

- And for you who are in the private sector, I cannot stress enough how important your role is in helping make this vision a reality. My advice is to keep doing what you've been doing:
    - Listen to America's emergency responders, so you'll know what they need and how you can give what they need to them.
    - Comply with standards.
    - Support the "system of systems" approach.
    - Educate America on our technology capabilities.

- Push the envelope—define what can be done today, and where we can go tomorrow.

Q&A With Under Secretary Cohen

Under Secretary for Science and Technology (S&T)

Q Would these required state communications plans be related to the giving of grants?

A We are asking that each state and territory submit a communications plan by November 1 to ensure eligibility for PSIC grants. There will be a peer review process no later than March 31, 2008. We are hoping to accelerate the peer review process (possibly in January) to allow states earlier access to grant money.

Q Can you submit your plans before November 1? Does the evaluation process start immediately?

A Yes, evaluators will provide feedback as soon as possible.

Q Can you give me some mote details on OIC pilots for multi-band radios?

A Many industries, foreign, etc. partners have come to DHS with series of potential interoperable solutions. We will be sending out several Broad Agency Announcements (BAA) and have received unsolicited proposals from companies. Other transaction authority approaches involve just granting a one time contract to a non-traditional performer. The offer provides a 30 percent offset for taxpayers for Independent Research and Development (IRAD) towards that project.

Q What kind of interactions/arrangements do you have with the Department of Defense (DoD) and the Defense Advanced Research Projects Agency (DARPA)?

A Enabling legislation allows those agencies to access all Federal components. We are very involved with DoD and have already established a Homeland Security deputy.

Q How should the plans for interoperability comport with the Interactive Weather Information Network (IWIN) and IWIN's ultimate plans?

A Mutual coordination needs to occur at all levels. Once its extracts information from statewide plans, OEC will make sure this information is incorporated into the future IWIN game plan.

Q How are states affected by state-level interoperability review?

A Our aim is to provide guidance to states to look downward into local/tribal governments to ensure that they have a coordinated plan.

Remarks from Representative Dave Reichert
Member, Committee on Homeland Security, US House of Representatives

From left: Under Secretary Jay Cohen and Representative Dave Reichert

Beyond Technology Solutions

- Interoperability is not solely a technology problem that can be solved only with the "right" equipment or the "right" communications system. All of the critical factors for a successful interoperability solution—governance, SOPs, training and exercises, and usage, *in addition to* technology—must be addressed.

- Technology remains a critical element in addressing interoperability, and solutions must be aligned with the needs of emergency responders in the field. Any solution must be based on user needs and be stakeholder-driven.

- As new technologies are developed and interoperability policy and protocols are revised, planning for communications interoperability must be done with the foresight of developing plans and systems that are flexible and adaptable to an ever-changing environment.

- Strengthening interoperable communications requires a practitioner-driven approach. The planning, development, implementation, and testing of the system must be done with the input of those who are going to use the system—local, tribal, and state emergency response communities.

Standards Acceleration

- For years, standards have been delayed. Emergency responders could not purchase equipment that was interoperable, regardless of manufacturer. This is no longer the case.

- Today, voice and data standards are being completed faster than ever before. OIC and NIST have worked closely with practitioners, industry, and other government agencies to make this possible.

National Interoperability Baseline Survey

- Last year, DHS released the results of the National Interoperability Baseline Survey. It is the first-ever assessment of interoperability across the Nation.

- The Baseline Survey assessed capacities across a wide array of factors, founded on the five elements depicted in the Interoperability Continuum—governance, SOPs, technology, training and exercises, and usage of interoperable communications.

- The Baseline Survey found that about two-thirds of agencies report using interoperability to some degree in their operations. Another key finding showed that agencies tend to be more advanced in technology than in the other key elements.

Statewide Planning

- This year, the Department is focusing on improving statewide planning for interoperability. Each state and territory is required to submit a statewide interoperable communications plan to DHS by November 1, 2007. A statewide plan is required to be eligible for the PSIC grant program.

Grant Funding and Guidance

- To date, DHS has provided approximately $3 billion to local and state governments to help them improve interoperable communications. More funding will be available this year through the Homeland Security Grant Program (HSGP) and the PSIC grant program.

- Coordinated grant guidance was developed to provide consistent criteria for agencies when purchasing equipment with Federal funds. The guidance helps maximize the efficiency of grant dollars allocated and spent on emergency response communications.

- The guidance represents the first time every communications-related grant agency in the Federal Government has incorporated the same criteria for agencies receiving Federal funds for interoperable communications.

Breakout Series I: Session A
Grant Guidance: What You Need To Know

Session Synopsis
Since 2003, DHS has provided approximately $3 billion for state and local communications interoperability initiatives, making it the largest category of expenditure through the Department's Homeland Security Grant Program, or HSGP. To ensure this funding is maximized by the state and local emergency response community, the Department carefully develops guidance and requirements for the funding. This guidance includes applicant and activities eligibility, application criteria, and recommended guidelines for equipment acquisition.

In this session, participants were given the opportunity to learn more about the Federal Fiscal Year (FY) 2007 interoperable communications grant programs and the accompanying guidance and requirements. Those who attended the session were also encouraged to provide recommendations for how industry can partner with the emergency response community to maximize the use of resources, including grant funding, in line with the "system of systems" approach.

Grant Guidance Panelists (from left): Scot Kelberg, Laura Pettus, Tony Frater

Panelists
Panelists included representatives from DHS OIC and the Federal Emergency Management Agency (FEMA), along with a representative from the US Department of Commerce who is heavily involved in public safety interoperability initiatives:

- **Tony Frater,** *Deputy Director, Office for Interoperability and Compatibility, DHS*
- **Scott Kelberg,** *Director, Technical Assistance Division, Capabilities Division, Federal Emergency Management Agency, DHS*
- **Laura Pettus,** *National Telecommunications and Information Administration, US Department of Commerce*

Session Key Points

- Interoperability is a multi-billion dollar problem. Not all communities are capable of dedicating the required resources needed to address the problem.

- As long as the emergency response community needs to communicate, significant funding will be needed to ensure that it is possible.

- Even if the problem was "solved" today, money and resources are still needed tomorrow for future planning, management, training, and maintenance, among other things.

- The Federal Government has made a concerted effort, through grant programs, to provide needed funding and guidance to state and local communities to address this critical issue.

- To ensure that funding dollars are maximized, coordinated grant guidance has been created which outlines recommended grant funding eligibility—including applicants and activities, application criteria, guidelines, and resources.

- The panel highlighted grant programs that support interoperability which are offered by:
    - National Preparedness Directorate of DHS
    - National Telecommunications and Information Administration (NTIA) of the Department of Commerce

- In the past, DHS has provided significant funding for interoperable communications. It is doing so again this year through the following initiatives, among others:
    - HSGP (Homeland Security Grant Program)
    - Infrastructure Protection Program (IPP)

- This year, NTIA is partnering with DHS to manage PSIC, the Public Safety Interoperable Communications Grant Program, which will provide approximately $1 billion to states and territories for interoperable communications activities.
    - To receive funding through this program, states will be required to develop and adopt statewide communications interoperability plans.

- NITA is working with DHS to release by the end of July a grant formula with a simplified application form.

- States and territories need to submit statewide interoperability communications plans and investment justifications by November 1, 2007.
    - If applications are not approved, guidance is given to improve applications.
    - No solutions are dictated.

- SAFECOM developed grant guidance to maximize the efficiency with which grant dollars related to interoperable communications are allocated and spent. The guidance outlines recommended grant funding eligibility—including applicants and activities, application criteria, guidelines, and resources.

- This was originally developed because multiple grant programs across the Federal Government provided funding for interoperable communications yet did not use common requirements or guidance.

- The guidance was developed with practitioner input, is based on a "system of systems" approach to interoperability, and takes into account each lane of the Interoperability Continuum—i.e.: governance, SOPs, technology, training and exercises, and usage.

- The guidance is updated yearly to account for programmatic developments. Highlights of this year's updates include:
    - Inclusion of criteria for the development of statewide interoperability strategic plans.
        - The Public Safety Interoperable Communications Grant Program will require that states develop and adopt such plans.
        - SAFECOM developed the statewide criteria in line with this requirement.

    - Updated Project 25 (P25) Information
        - Reflects developments in the P25 suite of standards.
        - Recommends that grant recipients purchasing P25 equipment be required to obtain documented evidence from the manufacturer that the equipment has passed all of the applicable P25 compliance assessment test procedures.
        - It should be noted that, as in past years, P25 is recommended as the standard for interoperable communications equipment. However, SAFECOM's guidance does not preclude the purchase of non-P25 equipment when there are compelling reasons to do so.

    - Language to account for the pursuit of current and next generation interoperability technologies such as gateways and backbone technologies that connect existing radio systems.
        - This includes, but is not limited to, IP-based solutions.
        - It is recommended that any such solutions are P25-compatible.

    - Starting in FY 2008, OEC, the Office of Emergency Communications, will be managing the development of SAFECOM's grant guidance. OIC will work closely with OEC to incorporate standards-related elements of the guidance.

FY 2007 Grant Programs

Homeland Security Grant Program (HSGP)

- State Homeland Security Program
- Urban Areas Security Initiative Program
- Law Enforcement Terrorism Prevention Program
- Metropolitan Medical Response System
- Citizen Corps Program

Infrastructure Protection Program (IPP)

- Transit Security Grant Program
- Port Security Grant Program
- Intercity Bus Security Grant Program
- Trucking Security Program
- Buffer Zone Protection Program

Other Programs

- Emergency Management Performance Grants (EMPG)
- Nonprofit Security Grant Program (NSGP)
- Competitive Training Grant Program (CTGP)
- Assistance to Firefighters Grants (AFG)
- Commercial Equipment Direct Assistance Program (CEDAP)
- Public Safety Interoperable Communications Program (PSIC)

Homeland Security Grant Program (HSGP) Risk Methodology

- DHS considers population in an area and the characteristics that might contribute to its risk, such as:
    - Intelligence community's assessments of threat
    - Population size/density
    - Economic impact of an attack
    - Proximity to national critical infrastructure

- Threat is based upon the intelligence and law enforcement communities' best assessments of which areas of the country—and specific targets—are most likely to be attacked.

- Additionally, they assess the national significance—and potential consequences—of potential targets.

About NTIA

- NTIA is responsible for the development of domestic and international telecommunications and information policy for the Executive Branch, and for ensuring the efficient and effective use of the Federal radio spectrum.

- NTIA has partnered with DHS, and has acquired the grants-related administrative services and expertise from the DHS Office of Grants and Training for the PSIC Grant Program. NTIA retains the approval authority on the program guidance, all grant awards, and grant applications.

Background on Public Laws

The Deficit Reduction Act of 2005:

- Established firm deadlines to complete digital television transition and return analog television spectrum, of which 24 MHz has been reallocated for public safety use.

- With the anticipated auction proceeds, NTIA was given authority to expend $1 billion in grants to public safety agencies to improve interoperable communications.

The Call Home Act of 2006:

- Established a deadline of September 30, 2007 to award PSIC grant funds.

PSIC Grant Program

The PSIC program assists public safety agencies in the acquisition of, deployment of, or training for, the use of interoperable communications systems that use the 700 MHz frequency band or enable use with the reallocated public safety spectrum.

- A 20 percent in-kind and/or cash match is required for this grant program. The grant will have a pass-through requirement to fund the projects of local public safety agencies.

- The applicants will have to complete three items to apply for the funds:
  - Simplified application (due in mid-August)
  - Statewide interoperability plans (due November 1)
  - Investment justifications (due November 1) that describe how the funds will be used.
- In the grant guidance, NTIA will encourage the use of innovative technical approaches, such as advanced technologies, spectrum-efficient solutions, and cost-effective measures.

Session Recommendations:

How can industry partner with the emergency response community to maximize the use of resources, including grant funding, in line with the "system of systems" approach?

- More education from Federal sources to the local emergency responder communities on grant programs and technology that meets grant requirements.
- Work with associations to provide information to the user base.
- Industry needs to help educate the public safety community of appropriate industry solutions that meet grant guidance requirements.
- Public Safety Wireless Network (PSWN)-style meetings to provide more forums of exchange between users and vendors. Users could describe lessons learned from system build-outs to provide users and vendors more information.
- More interaction between funding providers, users, and various vendors sponsored by DHS/OIC or NTIA.
- Define the emergency response community more broadly to include all organizations in emergency response (hospitals, 911, critical infrastructure, utilities).
- Use a cost-benefit analysis of interoperability for dollars spent. Work together to measure cost effectiveness.
- Link legacy and newer systems together, including public safety and broadband systems.
- Grant guidance should include standardized technology solutions.
- Provide free or no cost licensing of interface standards.
- Connect innovation with grant programs (R&D cycle).

Grant Guidance – Q & A

Q Are the statewide plans that need to be submitted the same plans that need to be submitted for DHS requirements?

A *Pettus:* Yes, they are now connected.

Q Is the SAFECOM vision represented in the statewide grant guidance?

A *Pettus:* We are working closely with SAFECOM and we do follow the statewide grant guidance.

Q Does NTIA have the final approval on guidelines and awards?

A *Pettus*: Yes.

Q There is an impetus within SAFECOM to follow guidelines, but it is technology-agnostic, is that correct?

A Yes.

Q Does grant guidance make it clear that it includes that ability to acquire software, etc. as opposed to only traditional methods of providing funding for land mobile radio (LMR) systems?

A The different fee services, operating expenses, etc. are options that are available under PSIC.

Q You mentioned three remarkable programs under DHS that are underutilized and not understood at the state and local level. Has the idea of a minimum level of participation in these programs been considered as a pre-requisite for receiving grant awards?

A *Kelberg:* SAFECOM grant guidance wouldn't promote it, because it is not focusing on one solution or technology.

A *Frater:* The focus is on two areas: incident-level communications and operability.

Q What are your plans to include specific language in grants to make agencies aware that the grants are applicable for spending on satellite systems?

A We have plans to do so within the next year or so. Currently we are trying to make it more clear through discussions and other interactive media

Q When are the statewide plans due? When will the awards be made? Do states and local agencies get money? Is it in 2009 or 2010?

A States and territories applying for PSIC grant program funding must submit final Statewide Communication Interoperability Plans (SCIPs) on November 1, 2007. In addition, states and territories have the option of submitting a preliminary plan no later than September 30, 2007. Though applications are due in the fall, the funding awards will be determined by DHS in mid-July 2007. At that time, states and territories will be able to spend up to 5 percent of their total award on planning activities associated with the development of their SCIP. Awards will be obligated to states and territories by September 30, 2007. States and territories will be able to spend the remaining 95 percent upon review and approval of their investment justifications and SCIP. The PSIC Grant Guidance and Application Kit, scheduled for release in mid-July, will provide more guidelines on how funding is to be distributed among state and local agencies, as well as guidance for submitting applications, investment justifications, and SCIPs.

- The Call Home Act requires that PSIC grants be allocated according to a DHS risk algorithm by September 30. However, states are only able to spend 5 percent of those allocated funds (for planning) until they have submitted and received approval on a statewide plan. At that time, they can begin spending the other 95 percent.

Q Homeland security met with states to cover statewide planning—who showed up? What was discussed? Are all states committed? Are you going to get a few useful plans? Who will need help?

A *Frater:* Fifty-two states and territories were present—all but four showed up. Up to five people per state were paid for, but more could have come. The event was a two-and-a-half day conference/workshop in which we spent time in teams going through different components of their plans and worked through the Continuum. Participants worked with other people from their region to share lessons learned and updates from statewide planning processes that were already being created or implemented.

- The hurdle is that this is a statewide plan, not a state plan. It needs to be a practitioner-driven statewide plan that incorporates local perspective.

A *Kelberg:* People were very enthusiastic coming out of the workshop.

A *Pettus:* NTIA was there and we were very impressed with what was happening. This will be an interactive process and the outcome will be a usable planning document, not something to stick on a shelf. The intent is to help the states, not shove Federal mandates or requirements at them that go without support.

Q Some localities have never seen a grant application nor read grant guidance, but 80 percent of money goes to locals and doesn't stay with the state if no Memorandum of Understanding (MOU) is involved. Who educates locals on money distribution methods and grant requirements?

A The leadership of the state needs to develop this. DHS has people in its offices that can help because they know local issues as they have been on the ground and are familiar with the process in localities. States also need an outreach program and a leadership initiative at the state level.

Q Have you have seen evidence of conformance within standards?

A *Kelberg:* Hopefully key components of the standards will be tested by August. Standards should be tested long before grant dollars come next year.

Q Is the supplier's declaration that "standards are met" sufficient?

A It is sufficient if the purchase needs to be made before standard completion. A more formal declaration of standards compliance will be possible after formal testing is done and then compliance assessment can be finished.

Q Homeland Innovative Prototypical Solutions (HIPS) and High Impact Technology Solutions (HITS) deadlines have past. Is money still available?

A Applications are vendor-neutral. Since providers have not yet received their funds, the opportunities may still be present.

Q There is an expanding range of technologies, not just equipment, software, services, etc. If someone comes in with a service that includes more than just interoperability, is there anything within grant guidance that precludes a service, or provider?

A The grant process promotes the widening of the net. Anyone who is in your interoperability plan and provides some solution needs to be considered as an acquisition partner.

Q Strategic technology set aside $100 million of the one billion dollars to create regional stockpiles—are you taking this possible legislation into account?

A *Pettus:* We are certainly considering all bills and congressional intent that is out there. If we fit it in the current program and statutorily do so while also meeting the September deadline, then we certainly consider those bills.

Breakout Series I: Session B
Emergency Interoperable Data and Messaging Standards Efforts

Session Synopsis

As new technologies spur the development of sophisticated but proprietary features, the user community struggles to benefit without heading down paths that lead to incompatibility. Representatives from three groups (practitioners, industry, Federal Government) are attempting to balance innovation with interoperability in the world of data and messaging standards development.

This session allowed attendees to learn the purpose and values of these efforts, explore what each of the three groups can bring to the table, and discuss the status of data and messaging standards adoption and implementation. Session participants created a list of recommendations for how industry can support the development, adoption, and implementation of these standards.

Standards Panelists (from left): Donna Roy, Mike Daconta, Paul Wormeli, Elysa Jones, Theresa Lynn Hadden, and Chip Hines

Panelists

Panelists included representatives from government, public safety, and industry who participate in standards development.

- **Chip Hines,** *Program Manager, Disaster Management Program, DHS*
- **Donna Roy,** *Director, Enterprise Data Management Office, DHS*
- **Mike Daconta,** *Vice President, Enterprise Data Management, Oberon Associates, Inc.*
- **Paul Wormeli,** *Executive Director, IJIS (Integrated Justice Information Systems) Institute*
- **Elysa Jones,** *Chair, Organization for the Advancement of Structured Information Standards, Emergency Management Technical Committee; member of the Emergency Interoperability Consortium (EIC), and Program Manager, Warning Systems, Inc.*

- **Theresa Lynn Hadden,** *Senior Application/Information Architect for Fairfax County, VA; Project Lead, National Capital Region Data Exchange Hub*

Key Points

The purpose and value of standards development:

- Partnerships produce standards.
- Standards should be driven by EMERGENCY RESPONDERS.
- Standards are good for business; there is economic viability for vendors to have uniform standards.
- Must organize our standards at the Federal level.
- Governance is critical for success in the standards arena.

The roles of Federal Government agencies and organizations in standards development for emergency responders:

- Disaster Management
- Enterprise Data Management Office
- IJIS Institute and the National Information Exchange Model (NIEM)
- Organization for the Advancement of Structured Information Standards (OASIS)

General Standards Information:

- An information exchange repository is needed, and we have begun to address this need.
- The DM or Disaster Management program works with a majority of the applicable data and message standards efforts, and has been working to assist the related standards.
- DHS recognizes that standards help interoperability; thus it has been striving to speed up the processes that bring standards through to product development. The development process begins with requirements from practitioners, and proceeds through internal research, formation of a standards working group, development of drafts, and submission of those drafts by the Emergency Interoperability Consortium (EIC) to OASIS for formal standards adoption.
- DHS and NIEM work involves MESSAGE standards for the exchange of information about resource needs (e.g., a need for generators).
- We need to look at some of the issues that surround the creation of the messaging and data standards. Examples are the business model, the stakeholders, and the degree to which the architecture is based on business processes first, and then the messaging and data.
- Technical assistance to aid in the understanding of standards like NIEM, Extensible Markup Language (XML), and Service Oriented Architecture (SOA) can speed their

adoption. It is recommended that industry retain neutrality in regard to technologies, and the ability to provide advice on standards that the practitioners should own.

- The EIC/OASIS process allows the vendor community to participate in and get visibility from the practitioners' work. Its standards are free and open to public.

- Vendors are encouraged to open their Application Programming Interfaces (APIs) to further the harmonization of standards at the national level. Governance and security are challenges.

Helpful Web Sites:

- Organization for the Advancement of Structured Information Systems (OASIS): *www.oasis-open.org*

- Emergency Interoperability Consortium (EIC): *www.eic.org*

- National Capital Region (NCR) Fire Resource Messaging System (RMS) Information Exchange Packet Documentation (IEPD): *http://www.ncrnet.us/demo-frri*

- NCR IEPD Clearing House: *http://it.ojp.gov/iepd/*

- NCR Development Toolkit: *http://www.ncrnet.us/deh/support_documents/NCR%20DEH%20Development%20Toolkit.pdf*

Emergency Interoperable Standards Q & A

Q Assuming technology is worked out, how do you address critical infrastructure that is sensitive but unclassified?

A *Daconta:* The Office of the Program Manager for the Information Sharing Environment (PM-ISE) is spearheading the effort to consolidate all the different Sensitive But Unclassified (SBU) classifications. We're looking at the 200 markings on sensitive information and simplifying them. A lot of work has already been done on access and identity management technologies (like those in the Homeland Security Presidential Directive (HSPD-12)), but there's a lot of work left to do. This presents the biggest opportunities and biggest challenge.

A *Jones:* The distribution element supports secure, multilevel content and uses a policy-oriented router. Also, some good tools are coming out that will help support the governance.

A *Hadden:* The two issues are: 1) we can't use large central databases—they must be local and distributed; and 2) we need to move quickly. The money is coming out now. We need identity management now.

A *Wormeli:* The PIMC is addressing the SBU classification under the rubric of counterterrorism. The 100 different SBU categories came from stovepipe policies and this doesn't touch other classifications such as DOD, Secret, and Top Secret. At present, we have the directive to solve the harmonization only for the SBU category. There are other issues as well (e.g., what do fusion centers share?).

Q Are there other standards than CAP we should know about? How do people get involved?

A *Jones:* First there was the Common Alerting Protocol (CAP) 1.0 in April of 2004. Then CAP1.1 addressed issues from the field. CAP is implemented around the world and currently the National Oceanic & Atmospheric Administration and the National Weather Service are looking at it. It is used for alerts and warnings. The International Telecommunication Union (ITU) will adopt it.

- Emergency Data Exchange Language (EDXL) resource messaging is now out for public review until June 8. Information on this is available on the OASIS Web site.
- Hospital AVailability Exchange (HAVE) is also coming along nicely. It is out for a 60-day public comment cycle; we have already received over 60 comments.

A *Hines:* EIC is one way you could get involved to hear about what's going on and check for feasibility. We go to the EIC for vendors for demonstration projects.

- OASIS has a number of vendor organizations. If you have practitioners in the area, let them know. Have them tell vendors to get the word out.

A *Wormeli:* For content standards go to www.niem.gov, and be sure to subscribe to the newsletter. There are lots of opportunities to serve on the committees. If any of you are interested, please contact us.

Q Industry has different views about standards. What do you think? What are the barriers to further adoption of them?

A *Hadden:* Most vendors will embrace standards, but there are economic challenges. For example, vendors need incentives and customers require standards. There's a tactical, quota-driven reality and vendors need to know someone's going to buy it.

- Word must really get out. There's a disconnect between government and what's in writing from the local purchasers.

A *Wormeli:* There's grant guidance requiring NIEM, so vendors must reach out to state and locals that are also buying.

A *Hadden:* They may need to use clearer language.

A *Roy:* The Department of Justice (DOJ) and DHS are affecting enterprise architecture such as the requirement for enterprise service bus (ESB) and trying to be NIEM-compliant.

A *Daconta:* I helped support the Transportation Security Administration (TSA) by putting it in contract language. There's a conflict of interest between vendors and standards: if you implement them, you make yourself plug and play.

- There must be cohesion between the purpose of the design and the standard. It is pretty simple to understand why CAP is accepted. Standards must be aware of the needs of implementers.

Breakout Series II: Session A
P25/CAP: What Does it All Mean?

Session Synopsis

Since the 1970s and the advent of digital signaling, manufacturers have incorporated proprietary protocols in their LMR, or land mobile radio, system products. As a result, interoperability among radio systems became a problem. In response, the Association of Public-Safety Communications Officials (APCO), with the support of several public safety organizations, Federal agency radio users, and industry, launched P25, or Project 25, in 1989. P25 is an effort to develop a suite of open standards that define eight interfaces for an LMR system.

- For backward compatibility, P25 radios can communicate in with legacy analog radios, and in either digital or analog mode with other P25 radios.
- The deployment of P25-compliant systems will allow for a high degree of equipment interoperability and compatibility, and will eliminate users being locked into having to purchase proprietary radio systems.
- In addition, DHS OIC is working with the Project 25 Steering Committee to establish a P25 Compliance Assessment Program (CAP). The program will begin assessing test laboratories for competence this September, and is intended to ensure that only P25-compliant equipment will be marketed.

The P25/CAP session consisted of formal presentations. It spurred large group discussions that provided participants with status and next steps regarding the P25 standards development and the establishment of the CAP. The session aimed to:

- Increase the understanding and transparency of the P25 interface standards development process.
- Clarify the progress of P25 interface standards development.
- Highlight issues affecting the development of P25-compliant products.
- Increase participant understanding of the program components and status of CAP.

P25 (from left): Eric Nelson and Dereck Orr

Panelists

Two experts on Project 25 standards development and compliance efforts served as session panelists:

- **Dereck Orr**, *Program Manager, Public Safety Communications Systems, National Institute of Standards and Technology (NIST)* led the P25 portion of the session.
- **Eric Nelson**, *Electronics Engineer and Team Leader of the Interoperability Research Laboratory, Institute for Telecommunication Sciences (ITS)* led the CAP portion of the session.

Session Key Points

- P25 consists of a suite of standards that define eight interfaces for an LMR system. Work has been accelerated on four of these standards because they have the largest role in assisting interoperability among emergency responders and public safety agencies. Of these four interfaces, the Common Air Interface (CAI) and the Inter-Radio Frequency Subsystem Interface (ISSI) are key to establishing interoperability.

- Each P25 interface comprises a suite of five document types: 1) overview documents; 2) protocol documents; 3) conformance test procedures; 4) performance test procedures; and 5) interoperability test process and procedures. An interface is considered complete when all documents for the five document types are published.

- Work proceeds on the test documents for the four accelerated interface standards with CAI and ISSI nearing completion.

- The following are definitions and status of each of the four priority P25 interface standards:

    1. **Common Air Interface (CAI)** – Defines the standards for over-the-air compatibility between mobile and portable radios (i.e., radio-to-radio) and between mobile and portable radios and tower equipment (e.g., fixed base station or repeater).

       Status: Critical steps are completed, and equipment is commercially available. CAP has been established to ensure equipment correctly implements Phase 1 standards, which are for 12.5 kHz-based equipment. Phase 2 standards, which are for 6.25 kHz-based equipment, are still in development.

    2. **Inter-RF Subsystem Interface (ISSI)** – Defines the wired interface to allow connection of one LMR system to another system, enabling them to act as one larger system. The result provides contiguous coverage and seamless roaming when the different networks work together.

       Status: Overview, protocol, conformance, and performance test documents have been completed. Conformance and interoperability test procedures are slated for fall 2007.

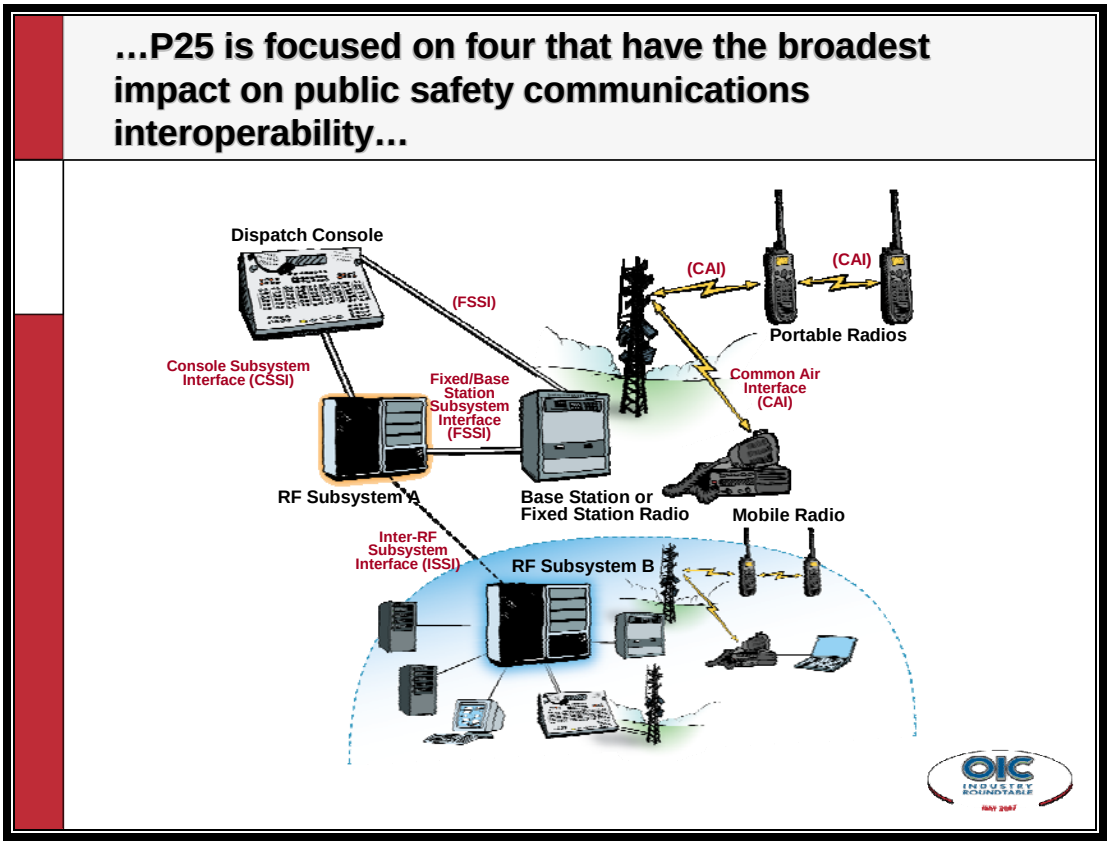
    3. **Fixed/Base Station Subsystem Interface (FSSI)** – Provides a standards-based signaling and messaging interface between the fixed/base station and the entire

LMR system, allowing users to purchase products of multiple vendors and use them seamlessly within their own system

Status: Overview, protocol, and conformance test documents have been completed.

4. **Console Subsystem Interface (CSSI)** – Provides a standards-based signaling and messaging interface between the console and the entire LMR system, allowing users to purchase multiple vendor products and use them seamlessly within their own system

   Status: Overview and protocol documents have been completed.



The P25 Compliance Assessment Program (CAP)

- To hasten the progress of P25 standards implementation and the public safety community's transition to P25, DHS grant policy states that grantees are expected to procure P25 equipment. Exceptions are granted if compelling reasons for using other solutions exist, such as when the interoperability of a legacy system would be compromised if new P25 equipment were introduced.

- The P25 CAP that is referred to in grant guidance is a first-party declaration of compliance with rigorous oversight—a formal process is now being developed and finalized.
  - P25 participants realize that there will be a learning curve associated with implementing this program, so outreach to equipment manufacturers and the

public safety community will be a priority. To facilitate program kick-off, NIST and OIC are working with P25 manufacturers to finalize CAP processes and procedures, and to capture these in a NIST handbook. Following this step, training will be performed with the manufacturers, and educational materials will be made available to the public safety community.

Resources for P25
Below are additional informational resources on P25, as well as the associated Web addresses:

- Decision Tree: Assists users in determining all features that need to be included in an Request for Proposal (RFP) when procuring P25 systems
  - *http://www.its.bldrdoc.gov/resources/p25/p25docselectionpublic.pdf*
- Department of Commerce ISSI Evaluation and Test System (DIETS): A downloadable tool that helps manufacturers in the development of ISSI-compliant systems, thereby ensuring that these interface standards are implemented consistently:
  - *http://snad.ncsl.nist.gov/proj25/*

Highlights of P25 Presentation
Dereck Orr, Program Manager, Public Safety Communications System, National Institute of Standards and Technology (NIST)

- At the request of Congress, NIST and OIC began participating in the Project 25 effort. The goal of this participation is to accelerate public safety interoperable communications through the development of national voluntary consensus standards.

- Project 25 standards are focused on achieving the following goals that benefit the public safety community:
  - Graceful migration
  - Competition in systems lifecycle procurements
  - Interoperability
  - Practitioner-driven approach
  - User-friendly equipment
  - Spectrum efficiency
  - Robust compliance assessment program

- The CAI standards have become more defined during the last few years, resulting in a more mature set of documentation for this interface.

- ISSI is a key to interoperability in that it allows roaming and overlap of coverage between different manufacturers' radio networks. It defines how different P25 trunked radio networks can connect with one another. Manufacturers are currently in the research and development phases as they begin to develop ISSI equipment.

Highlights of CAP Presentation
Eric Nelson, Electronics Engineer and Team Leader of the Interoperability Research Laboratory, Institute for Telecommunication Sciences (ITS)

- The goal of CAP is to establish a program that engenders a high degree of confidence in products marketed as P25-compliant and that minimizes the time spent testing products.

- As a result of lab testing, implementation issues were discovered in which Subscriber Units (SUs) did not comply with the standards. These results pointed to the need for a program to assure users that an objective analysis of SUs has been completed and that equipment advertised as P25-compliant indeed meets the standards.

- The CAP program was established to promote and ensure P25 equipment compliance with standards. CAP is not a certification program. Instead, it consists of a Supplier's Declaration of Compliance (SDoC), backed by rigorous testing with independent oversight. Public safety users will have access to summary test reports generated following testing. Detailed test reports which substantiate standards compliance will be signed by a responsible company official providing a high degree of accountability.

- CAP will leverage conformity assessment standards already developed by internationally recognized standards bodies. NIST is in the process of creating a user handbook for the program patterned on these best practices.

- Several of the performance tests defined will not be critical for manufacturers to perform; however, features that affect public safety users must be tested.

CAP Auditability

- Independent labs or manufacturers will be subject to periodic reviews.

- Product change control logs are recommended for participating P25 manufacturers.
    - For any system update introduced without a full regression test, a rationale will be provided.

Definition of Compliance

- A minimum set of tests will have to be completed in order for a product to be considered "P25-compliant."

- Going forward, the Compliance Assessment Process and Procedures Task Group (CAPPTG) will make recommendations to the P25 Steering Committee of which test cases constitute compliance.

Suppliers Declarations of Compliance (SDoC)

- SDoC is a formal declaration of compliance with standards. A P25 SDoC will list the test procedures that were successfully accomplished on a product
    - All declarations will be posted in a repository.
    - A summary test report for interoperability testing will detail product revisions and identify all SUs that are tested against it.

- All product details will be listed with enough information so that users can purchase the product with a sufficiently specified configuration.
    - Testing procedures are being formalized by Project 25

Test Development

- The first phase of the program is limited to performance and trunked voice interoperability testing for the Common Air Interface.

- Manufacturers desire a rigorous process that examines the test process and includes a more comprehensive lab checklist.

- A set of documents will be published in the near term that will expand the number of test procedures required to demonstrate compliance as more compliance assessment test procedures are published.

- Test lab assessment is planned for fall 2007. Lab assessments will ensure a rigorous testing process is implemented that is accurate and repeatable.

Questions to be Addressed
Session attendees identified the following questions they would like to see addressed in a future posting of P25 CAP Frequently Asked Questions (FAQs) (These questions and their answers will be posted on the OIC Web site):

- When is the CAP program expected to begin?

- Which P25 standards and testing aspects will grant guidance address?

- What specifically is required to comply with grant guidance?

- Is there intent to unify the DHS and the SAFECOM grant guidance documents?

- How soon will grant guidance be unified into a single document?

- What can users do now to ensure procurement of P25-compliant radio systems?

- When are the other interface standard documents scheduled to be completed?

- Will quarterly reports and timelines concerning CAP milestones be available?

- What consequences will there be to manufacturers for equipment they claim is P25-complaint, but which testing indicates is not?

- What are the differences between first-, second-, and third-party testing, and what timelines apply for each?

- Where are/will compliance test results/information be posted and available to the public safety community?

P25/CAP – Q & A

Q You mentioned that the program kickoff will be this summer. What does "up and running by the end of this year" mean?

A The following milestones have been set: Training for laboratory assessors with subject matter expertise is planned for July 2007 to ensure they follow internationally accepted practices while conducting assessments. Coordination and interaction with labs will take place this summer so they are prepared for initial lab assessments by early Fall 2007. Following these assessments and laboratory recognition, reports are expected to be available by in late fall or early winter 2007.

Q When do you expect to turn attention to ISSI? How much of the process and concept that you are using with CAI will carry over to ISSI? And CSSI – will you turn your attention there as well?

A The CAP is not specific to any interface. Testing is predicated on the development of product and associated compliance assessment test procedures. Once these are available the process of assessing labs will be initiated with lab recognition and test reports expected to follow soon thereafter.

Q From a user perspective, what is it that we're going to be getting in terms of the CAI and then the ISSI?

A CAI allows multiple manufacturers to build SUs that will work with multiple systems—not locked into one manufacturer. With P25, the talk around mode can be accomplished independent of the manufacture of the SU. SUs under specific conditions can be incorporated into another system and work with all of the features.

- ISSI allows SUs to roam on to other systems, operating on a different band or regardless of manufacturer.
- FSSI allows for expansion of a system using equipment from any manufacturer. The result is that the user is not forced to purchase fixed stations from the same manufacturer. As such, these standards encourage competition, price reduction, development of a range of features, and the incentive to address public safety user requirements.

Breakout Series II: Session B
VoIP: What it Can Be

Session Synopsis

Over the past year, OIC, along with its Federal partner, NIST's Office of Law Enforcement Standards (NIST/OLES), assisted with roundtables between public safety and industry about Voice over Internet Protocol's (VoIP) role in emergency response communications. Participants in this session gathered insights from these roundtables and weighed in on next steps.

Panelists discussed:

- The role and opportunities for VoIP in the emergency response environment
- The requirements of emergency responders with respect to VoIP
- The collaborative efforts currently underway to advance development of VoIP emergency response interoperable standards

Session participants had the opportunity to make recommendations for ways in which industry can work with the emergency response community to enable the use of this technology.

VoIP Panelists (from left): Captain Robert Kuzma, Linda Fuchs, Luke Klein-Berndt, and DJ Atkinson

Panelists:

- **DJ Atkinson**, *Lead Electronics Engineer, National Telecommunications and Information Administration (NTIA), Institute for Telecommunication Sciences (ITS)*

- **Linda Fuchs**, *Program Manager, Department of Management Services, Enterprise Information Technology Services, State of Florida*

- **Luke Klein-Berndt**, *Chief Technical Officer, Office for Interoperability and Compatibility, DHS*

- **Captain Robert Kuzma**, *Technology Implementation and Risk Assessment, San Francisco Fire Department*

Session Key Points:

- One concern of emergency responders is the current inability to connect VoIP products to each other in the absence of interface standards.

- The issue with emergency responders' use of VoIP is not just technology, but *governance, consensus,* and *political issues*.

- Users don't care *what kind* of technology works; they just want it to work.

- Education is important—NIMS training is vital

- OIC and NIST/OLES are working with industry and emergency responders to develop implementation profiles for VoIP in each of the following environments:

    - Emergency Response Environments for VoIP
        - Bridging Systems Interface
        - Radio Site Interface
        - Radio System to Radio System Interface
        - Dispatch Interface
        - System to Subscriber Unit (Last Mile Radio)
        - Wired End Unit to System Interface

    - Emergency Response Requirements for VoIP
        - Interoperability, compatibility, interchangeability
        - Minimum set of standards and features
        - Common security framework
        - Reliability
        - Affordability
        - Scalability
        - Manageability
        - Education/Training
        - Leverage Commercial Off The Shelf (COTS) products
        - Ability to compare VoIP offering to other alternatives to meet public safety functional requirements

- Florida has been using VoIP for some time, and has encountered little resistance. The largest implementation is the Florida Interoperability Network (FIN), which boasts mutual aid channels with phone lines and repeaters. Its radio-over-IP network connects 150 radio systems and dispatch centers. It was built with DHS grant funding.
    - Aside from the integration of Nextel to FIN, Florida is also connecting it to Georgia's network. This connection, although reduced to a simpler technology, will help with border pursuits, fires across the borders, and evacuations. Standards would have made this connection a more "full-fledged tool".

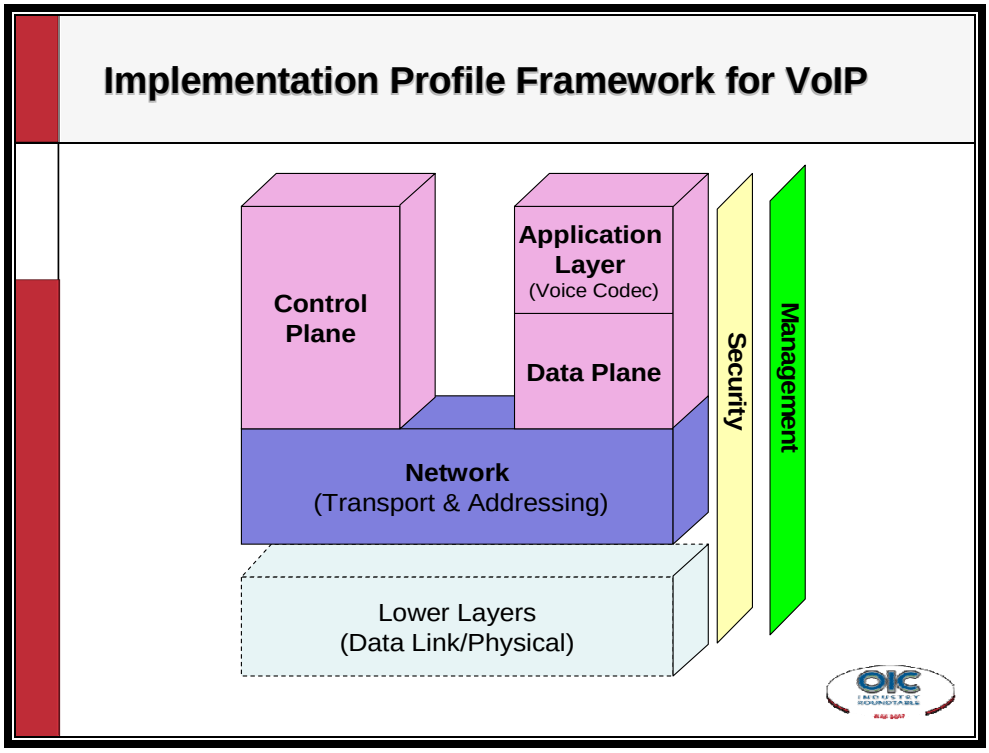
- FIN is extremely cost efficient: For $50/responder, personnel can go anywhere in the state, and talk to whom they need, either back home or with those they're assisting. Although each node is $11,000, the costs are divided amongst tens of thousands of responders across the state.
    - With a reliable network, and focus on their mission, most users don't know or care about the network itself. The key to implementation was the governance and the political will: "that's made the difference."

- There is weakness in the term "VoIP"…it means a lot, and nothing." For example, because it's based on IP, people assume it's inherently interoperable, but there's a dire

lack of commonality in implementation—not a lack of standards. People need to agree on which standards to use and how to use them.

- The implementation profile is a minimum set of standards, parameters, and values needed to assure interoperable communications.

- The 24-month goal is to finish an implementation profile for the bridging systems interface that is based as much as possible on previous work.



Breakout Recommendations

Question: What else can OIC do regarding VoIP in Emergency Response communications? What group(s) should OIC be engaging in this process?

- Determine what works and what doesn't.

- Specify where VoIP is being done—over the air or on the ground, gateways vs. backbones.

- Develop a consistent use of terms.

- Recognize that the solutions in the Continuum should not necessarily be ranked purely from left to right: Florida is using gateways and bridges as a part of its interoperability mix; however, with gateways low on the Continuum scale, the perception is that they are frowned upon. Even swap-radios can play a vital role in some scenarios. Make it clearer that the goal of interoperability funding is movement toward the right side of the Interoperability Continuum from where things currently stand.

- Draw on the experiences of states and localities along with other interested parties with similar features—particularly reliability, ubiquity, and security—in order to share best practices and come to shared understandings of important issues.

- People don't care about the technology; they just want to meet their tactical or strategic objectives.

VoIP Q & A:

Q What is the main vulnerability of the Florida Interoperable Network (FIN)?

A *Fuchs:* Its main vulnerability is the network itself, but with cooperation of the vendors, and redundancy throughout, it can now work around single points-of-failure.

Q What is the security like on Florida's network?

A *Fuchs*: Florida's network is encrypted, with an unencrypted layer for communication with "cooperators" like utilities, and someday perhaps, with citizens. Sensitivity to security concerns is paramount.

Q Linda, have you had products of different vendors?

A *Fuchs:* The focus is the radio system; the interface box is ONE vendor.

A *Kuzma***:** We, too, use products of one vendor so there's no pointing fingers and blaming the other vendor.

A *John Powell (National Public Safety Telecommunications Council (NPSTC)***:** Legislators don't realize it's the interface that needs to be compatible.

Q Kuzma was criticized for using a gateway, so why are you focused on them?

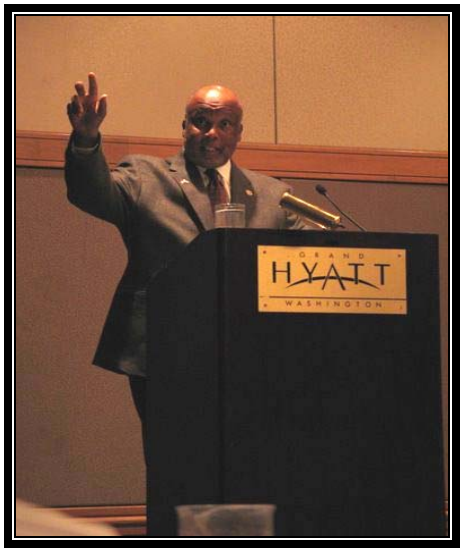
A *Kuzma***:** No, the issue is Federal Government guidance. Bridging solutions are "somewhat out of favor."

A *Klein-Berndt:* Guidance will be refined so that it won't appear as if any of the tools is looked down upon if it is the appropriate one for the task. The point is clear about a full suite of solutions, and the grant evaluations must match this.

A *Atkinson***:** Interoperability approaches should be evaluated on this factor: Does your proposal move you from where you are to where you want to be? Some vendors say "we have a solution" so long as you buy it from us. We're focusing on the interface between bridging devices so that users can have voice interoperability regardless of vendor.

Keynote Speakers

Representative Bennie G. Thompson
Chairman of the U.S. House of Representatives Homeland Security Committee



Representative Bennie G. Thompson

Beyond Technology Solutions

- Interoperability is not solely a technology problem that can be solved only with the "right" equipment or the "right" communications system. All of the critical factors for a successful interoperability solution—governance, SOPs, training and exercises, and usage, *in addition to* technology—must be addressed.
    - Review of interoperability in December showed that most areas are not working together to use the technology appropriately.

- Technology remains a critical element in addressing interoperability. Technology solutions must be aligned with the needs of emergency responders in the field. Any solution must be based on user needs and be stakeholder-driven.

- As new technologies are developed and interoperability policy and protocols are revised, planning for communications interoperability must be done with the foresight of developing plans and systems that are flexible and adaptable to an ever-changing environment.

Standards Acceleration

- For years, standards have been delayed. Emergency responders could not purchase equipment that was interoperable, regardless of manufacturer. This is no longer the case.

- Today, voice and data standards are being completed faster than ever before. OIC and NIST have worked closely with practitioners, industry, and other government agencies to make this possible.

National Interoperability Baseline Survey

- Last year, DHS released the results of the National Interoperability Baseline Survey. It is the first-ever assessment of interoperability across the Nation.

- The Baseline Survey assessed capacities across a wide array of factors, founded on the five elements depicted in the Interoperability Continuum—governance, SOPs, technology, training and exercises, and usage of interoperable communications.
    - The Baseline Survey found that about two-thirds of agencies report using interoperability to some degree in their operations. Another key finding showed that agencies tend to be more advanced in technology than in the other key elements.

Statewide Planning

- This year, the department is focusing on improving statewide planning for interoperability. Each state and territory is required to submit a statewide interoperable communications plan to DHS by November 1, 2007. A statewide plan is required to be eligible for the PSIC grant program.

Grant Funding and Guidance

- To date, DHS has provided approximately $3 billion to local and state governments to help them improve interoperable communications. More funding will be available this year through HSGP and the PSIC grant program.

- Coordinated grant guidance was developed to provide consistent criteria for agencies when purchasing equipment with Federal funds. The guidance helps maximize the efficiency of grant dollars allocated and spent on emergency response communications.

Assistant Secretary Greg Garcia

Assistant Secretary for Cyber Security and Communications (CS&C), Department of Homeland Security

Assistant Secretary Greg Garcia

- Prior to my appointment as the first Assistant Secretary for Cyber Security and Communications (CS&C), I was working in the private sector, and now, having served in both the public and private sector, I can truly appreciate the importance of the partnership among government, industry, and the emergency response community in achieving our homeland security goals.

Convergence and the Modern Communications Environment

- In the next 10 years or so, a single, advanced integrated IP network will be handling the majority of the world's communications needs. This converged broadband network will extend well beyond local and long-distance voice, video, and data. It will support an ever-widening array of services across a billion connected devices globally.
    - Our challenge is to ensure that these systems and services remain available, resilient, secure, and interoperable. That is the charge of my office, CS&C.

- CS&C was established to lead the Department's effort to ensure the security, resiliency, and reliability of the Nation's cyber and communications infrastructure in collaboration with the public and private sectors. We do this through three components:
    - The National Cyber Security Division, which fosters a public-private partnership for cyber security awareness, risk mitigation management and mitigation, and information sharing and incident response
    - The National Communications System, which coordinates the provision of national security and emergency preparedness communications for the Federal Government under all circumstances, including crisis or emergency, attack and recovery, and reconstitution
    - The newly created Office of Emergency Communications (OEC).

- These three components are working together to foster public, private, and international partnerships and to enhance the preparedness of our Nation's IT and communications infrastructures.

OEC

- In October of 2006, the U.S. Congress established the OEC within CS&C as part of the reorganization of the Department's emergency preparedness and response functions.

- OEC combines three critical interoperability programs from across the Department, including:
    - The policy, outreach, and planning elements of the SAFECOM Program
    - The Interoperable Communications Technical Assistance Program, or ICTAP, which works hand-and-hand with the states and localities
    - Parts of the Integrated Wireless Network, or IWN, which is a joint project with the Departments of Justice and Treasury focused on Federal interoperability

- We are looking to industry to develop the equipment and technologies that meet the defined requirements of the emergency response community, providing security, reliability, scalability, and affordability.
    - Innovation in meeting these requirements is needed not only for existing technologies, but also for the convergence from circuit-switched telecommunications to emerging technologies such as IP and Broadband.

- We are hard at work providing technical assistance to the states to help them prepare their statewide interoperability plans, which are due in the fall.
    - OEC will be a key participant in the FEMA peer review process to evaluate and approve the plans.
    - Once the states receive their PSIC grant, OEC will stand ready to provide them with additional technical assistance.

- Three key roles I see industry playing in this picture:
    - Supporting the “system of systems” approach to interoperability
    - Building equipment and technology that meets defined standards and requirements of the emergency response community
    - Developing innovative solutions for existing and future interoperable and emergency communications

- It is essential that industry engages in the development of standards not only for existing technologies, but also emerging technologies.

Breakout Series III: Session A
National Interoperability Baseline Study: So What?

Session Synopsis

In fall 2006, DHS delivered the results from the National Interoperability Baseline Survey, a mechanism that was used to determine and measure interoperable communications nationwide to improve their effectiveness for emergency response practitioners. This session provided participants with an understanding of the results of the Baseline Survey, clarity about its implications, and an opportunity to develop solutions to gaps that the study identified. Session participants were asked to provide recommendations for how industry can enhance its approach to interoperability solutions to support OIC and the emergency response community in closing some of these gaps.

Baseline panel (from left): Col. Victoria Velez, Marilyn Ward, Troy Cribb, Veronique Pluviose-Fenton, and Tony Frater

Panelists:

- **Colonel Victoria Velez**, *Director, Office of Emergency Communications, DHS*
- **Marilyn Ward**, *Executive Director, National Public Safety Telecommunications Council (NPSTC)*
- **Troy Cribb,** *Majority Counsel, Senate Committee on Homeland Security and Governmental Affairs*
- **Veronique Pluviose-Fenton**, *Majority Senior Counsel, House Committee on Homeland Security*
- **Tony Frater**, *Deputy Director, Office for Interoperability and Compatibility, DHS*

Session Key Points

Results of Baseline Survey:

- Fire/EMS and law enforcement agencies tend to show the same degree of development.
- State-local interoperability tends to be less advanced than cross-discipline and cross-jurisdiction.
- Small agencies tend to be at less advanced stages of development than larger agencies.

- Agencies that operate on large, shared systems tend to be at more advanced stages of development.

- Agencies are least advanced in the non-technology elements.

- Two-thirds of the agencies use interoperability to at least a moderate degree.

Implications of Baseline Survey:

- For Congress, the survey demonstrated that there is still a lot of work to do. It is important to continue to listen to the public safety community. Congress will focus on the principles of the Interoperability Continuum to guide future policy and grants on communications interoperability.

- The survey reinforces that this is not a technology issue, and it certainly helped to educate members of Congress of this. There is a need for more funding and there is a Federal role to step in and help.

- The Baseline Survey also demonstrates the value and need for a comprehensive national assessment that OEC will conduct.

- The results of the study are things the public safety community has known all along, and now the community has the results documented to help them communicate with Congress on their needs. Funding continues to be problematic for the public safety community. Even small amounts of equipment for incremental upgrades are expensive. Funding is critical and there aren't enough bodies to do the work.

- The Baseline Survey did capture some information on the use of data (text messaging, use of broadband, etc.) in emergency communications, however, the focus groups who helped create the survey deemed voice interoperability as the focus for this first ever baseline survey on interoperability.

- OEC will conduct a follow-up survey in two years and will look at the possibility of including more questions on data, video and text, etc. Interoperability includes all aspects of emergency communication, not just voice communications.

- The Baseline Survey solidifies the point of view that this is not a technology issue. Many public safety agencies see this arena as a technology issue, but it is really a much more complex issue—it includes all the other areas of the Continuum. This report is very good at reinforcing that fact.

- The study also reinforces the need for more funding. Everyone in this room knows that providing adequate and consistent funding in this area is a big struggle for states and localities. Federal help is needed, which is why we (Congress) are trying so hard to set up an independent grant program at DHS.
    - There are other grant programs set up, but many of us on the Hill believe that we really need a new one just dedicated to interoperability.

- The Federal Government needs to facilitate a dialog and coordinate with regions to ensure the input is from the bottom up. Progress reports and the baseline study will be able to give a clearer picture to Congress to aid in funding decisions.

Overall findings

- Fire/EMS and law enforcement agencies tend to show the same degree of development across three-quarters of the Continuum topics.
- State-Local interoperability tends to be at a less advanced stage than Cross-Discipline and Cross-Jurisdiction interoperability.
- Small agencies (whether measured by staff or population served) tend to be at less advanced stages of development than larger agencies.
- Agencies that operate on large, shared systems tend to be at more advanced stages of development than those that operate on stand-alone systems.
- Two-thirds of the agencies use interoperability to at least a moderate degree.
- Agencies have advanced less in the non-technical elements of the Continuum, particularly with respect to training, frequency of use, and standard operating procedures.
- 64 percent of agencies have some element of interoperability.
- Most agencies are in the early or moderate stage of interoperability.
- Frequency of use and familiarity with interoperable communications is one of the greatest determinants of success in achieving interoperability, and is thus one of the most important aspects on which to focus.
- For many agencies, funding for capital investments (one-time purchases) is an obstacle.
- Technology:
    - The vast majority of responding agencies indicated they also use commercial wireless telephones, wireless personal digital assistants (PDAs), or regular landline telephones/faxes to achieve interoperability. This demonstrates that first responders tend to use portable devices that are convenient and readily available in real time.
    - The relatively low percentage of agencies employing NPSPAC channels could reflect the prevalence of conventional systems in the field or indicate problems in programming or a lack of visibility for this solution.
    - Very few agencies indicated the use of deployable solutions—field interviews note a preference for seamless solutions as opposed to solutions that may be complex and time-consuming to establish.
    - More than half operate VHF systems for their primary system—these systems use older analog technology to cover large geographic areas while deploying less infrastructure than required by systems that operate in higher spectrum bands.
    - Over half indicated that they currently have sufficient spectrum to support mutual aid channels, while just 41 percent indicated that they have sufficient spectrum to support mutual aid channels for future operations.
    - Spectrum—both current and future availability—supporting broadband applications (e.g., sending photographs or e-mail) is deemed less sufficient.

Tony Frater, *Deputy Director, Office for Interoperability and Compatibility, DHS*

- The baseline helps to identify gaps and what tools and technology are in use. It also provides statistical evidence to support what agencies have been saying for years, and finally provides data to support their claims.

- The Baseline Survey, a random survey responded to by over 6,000 agencies, looked at three different levels of interoperability:
    - Between disciplines in the same jurisdiction
    - Same disciplines across jurisdiction
    - Multiple disciplines across jurisdictions

- The survey went to over 22,000 public safety agencies. Responding was completely voluntary. We had a 30 percent response rate, and a confidence rate of validity of data of over 99 percent. There was a great distribution of responses.

Colonel Victoria Velez, *Director, Office of Emergency Communications, DHS*

- We have a long way to go in terms of interoperability. We need to know where we are in order to build the road ahead for interoperability, public safety, and the Federal Government. A lot of work needs to be done. The Baseline Survey is a mandate and Congress wants us to develop a report to show how we are doing. We need to know the gaps and this survey will help us build a national inventory.

- Foundation documents will include the Baseline Survey, scorecards, tactical interoperable communication plans, and statewide plans. The survey is due October 1. In order to complete this correctly, we're asking for permission from Congress to do it in a two-phase plan.

- We need to further define the emergency response plan so that agencies can build their plans. We need to get information out of statewide plans to build a national baseline assessment.

- The assessment will ensure that we have an understanding of the range of both capabilities and gaps, seams, and obstacles. It will ensure that the Department is ready with an inventory so that we will know what equipment is available in each state and locale.

Veronique Pluviose-Fenton, *Majority Senior Counsel, House Committee on Homeland Security*

- From the Hill perspective, we have a lot of work to do. We have a lot of reasons to listen to the practitioners on why we should use this system. We have a direct pipeline of representatives who were former public safety responders and also have access to practitioner groups. The chairman will be very clear that technology itself is not the answer.

- It's very important to consider the other pillars of the Interoperability Continuum. We have an opportunity to ensure that the SAFECOM Interoperability Continuum serves as a guide on the road to interoperability for states and localities.

- There are going to be continual reasons to adapt and evolve to meet the needs of public safety interoperable communications. The chairman views the 911 implementation bill as an opportunity to solidify the use of the Continuum as a road to interoperability. We need a stand-alone grant at DHS to incorporate and build an office of emergency communications.

Troy Cribb, *Majority Counsel, Senate Committee on Homeland Security and Governmental Affairs*

- Many public safety agencies see this as a technology issue, but it really is so much more than that: it includes all the other areas of the Continuum. This report is very good at reinforcing that notion.

- The study reinforces the need for more money. Everyone in this room knows that this is a big struggle for states and localities, and Federal help is needed, which is why were trying so hard to get an independent grant program at DHS set up.
    - There are other grant programs set up, but we really need a new one just dedicated to interoperability.

- We need a facilitated dialog, coordinated with regions, to ensure the input is from the bottom up. Progress reports and the baseline study will enable us to give information to Congress to aid in funding decisions.

Marilyn Ward, *Executive Director, National Public Safety Telecommunications Council (NPSTC)*

- Funding is critical. There is no money, which means that communication managers have to compete against bullet-proof vests and other equipment (like fire trucks) that need to be purchased at a local level. You can't see radio waves, so people don't understand how much it takes to build out the equipment to use radios.

- $6 million was needed to build out three frequencies to use up and down the coast of Florida—a lot of money. This is why it can't be done across the rest of the country—the money isn't there. The grant dollars that have been coming down to the local people are really helpful because there isn't a requirement to compete and the money is allotted for vital communications. The funding is critical, as seen in Florida to build a "system of systems" approach.

- In an effort to provide assistance in the smaller agencies, the Federal Government has stepped up by conducting a baseline study that allowed localities to document the deficiencies. This allowed them to gain congressional support to gain funding to put into the localities.
    - While everyone calls this governance, it is really a people problem—it's difficult getting the leaders to come and play, there is a 30 percent turnover in dispatch centers, and it takes a lot of money to train people, both for backfill and current staff.
    - The guidance from SAFECOM, and the support from grants that ensure that people continue to work together, have been critical to do what we do at the local public safety level.

Baseline Q&A:

Q How were communications centers included in the baseline study? Readiness plans and interoperability plans are separate – this is a challenge for states and localities and this is a great opportunity to get these two things on track.

A *Frater:* I agree completely, it's hard to cap who and how you survey. There are a lot of very important people in the supply chain, but from a practical and resource perspective we capped the study to those three (law enforcement, fire service, and EMS) disciplines. In the future we could include communications centers.

A *Ward:* There are studies performed at the local level and they are available on the localities' Web sites.

A *Pluviose-Fenton*: Input from local and regional stakeholders is incorporated into the Federal operation emergency plan. Fragmented plans generate fragmented systems. Whatever the program the grants are from, there needs to be some consistency or an explanation why another need overrides that for consistency.

Q Is the idea that the funds will be administered to statewide administrators in order to push them down to localities?

A *Cribb:* For the $1 billion, the NTIA is taking the applications from the states and the grants will be used consistent with the statewide plans being submitted in October. We want the grants in the grant program to be used, but we don't want one or two states to gobble up all the money. The state will push the money down to localities.

A *Pluviose-Fenton:* There is a discussion as to whether it will be a risk phase or hazard phase. According to DHS, it will be a risk phase. This will include 911 and natural disasters. The funding determination will be made by September 30 of this year. The deadline date was moved up because NTIA and DHS did not get their MOU signed until February. You will know what you're getting by September 30; it's a multiple-year obligation process for states and locals.

A *Ward:* The local and state people will work together. There will be various coordinated efforts in regards to the RFP. A regional situation may have a consortium, but a state may need a RFP for equipment.

Q How are you ensuring that these efforts are not duplicating a UASI (Urban Areas Security Initiative) effort?

A *Cribb*: This is legislation we are working on right now. In the Senate bill, there is a provision that DHS needs to consider whether there are other funding sources. It may be appropriate to have two funding sources, but we should have language to indicate that an interoperability grant needs to consider other efforts.

A *Velez:* Interoperability includes everything that is used to communicate. We are currently focused on voice, but there is so much more. We need to make sure that all these methods are considered.

A *Ward:* Keep in mind that we need to get something solved with voice interoperability. And voice is mission-critical; it's our number one concern, although other methods need to be considered.

A *Frater:* The baseline did include other communication efforts, including text messages, laptops, etc. Also, we need to determine if it's worth the extra 15 or so questions to include in the survey. It took a lot to get the survey off the ground, but it is on our docket to include in the next survey in a year or two.

A *Pluviose-Fenton*: Congress has learned to change language from "state" to "statewide," and we're hoping DHS will encourage this all-encompassing messaging through its grant guidance.

Q How much interoperability is required among entities considering DoD's involvement? Will first responders be ensured priority access considering the large number of people that will need to be active on the systems?

A *Velez:* Interoperability needs to exist among all entities responding to an event. It is a work in progress. DoD always wants to be there when it can, but localities need to be interoperable with each other. Channel access and channel prioritization is something we need to articulate and define. I can't give you an assurance that prioritization will occur, but it's something we need to attain.

A *Frater:* A big component is training: who needs to talk to whom, when, and how. We're developing a NIMS training course so that this information will be available.

Q The writing of an interoperability plan is primarily focused on voice communications: what's being done to enforce the inclusion of data and video?

A *Frater:* The statewide planning guide that exists incorporates data: voice, data, video, etc.

A *Velez:* Governance, technology, SOPs, and training/exercises are all key areas that the state needs to look at for interoperability. There needs to be consistency across the states for inclusion of all these methods.

Q Many utilities need to be involved in incidents as well – what incentives have been provided for states to incorporate the extensive utilities network involved?

A *Ward:* Many of the states include utilities in the plan. There are a lot of partnerships out there, but the degree to which they are involved varies from state to state.

A *Frater*: We are addressing these issues. The guidance does include the involvement of all the entities that are associated. We are about to start a pilot to find efficient ways to bring other emergency responders into talk groups so that they can participate.

A *Pluviose-Fenton:* At a FEMA conference, we did specifically require that utilities be included. From my boss's perspective, he really doesn't like to have so much spelled out in legislation for fear of leaving someone out. We're hoping that the general framework allows the Department to take it and run with it and honor the spirit of the legislation. The more descriptive we get, the more it invites congressional parties to weight it based on their jurisdictional lines.

Breakout Series III: Session B
Public Safety Broadband: Can It Really Work?

Session Synopsis:
While "broadband" typically refers to high-speed data transmissions without regard to whether it is wired or wireless, the mobile nature of emergency response moves the focus to wireless, and its myriad applications. These range from text messaging and database access to telemetry and the detection of weapons of mass destruction. This session explored the networks and technologies that underlie wireless broadband, how these may develop in the future, and ways to pay for it. Representatives from public safety shared the challenges they've encountered, lessons-learned, and their requirements for tomorrow. Session participants were asked to give OIC a list of suggested recommendations moving forward.

Broadband Panelists (from left). Harlin McEwen, John Powell, Robert LeGrande II, David Boyd, Morgan O'Brien, Christopher Guttman-McCabe and Gregory Henderson

Panelists:

- **Dr. David Boyd**, *Director, Command, Control and Interoperability, DHS*
- **Morgan O'Brien**, *Co-founder and Chairman, Cyren Call Communications*
- **Christopher Guttman-McCabe**, *Vice President of Regulatory Affairs, International Association for the Wireless Telecommunications Industry (CTIA)*
- **Gregory Henderson**, *Manager of Broadband Technology, Tyco Electronics Wireless Systems Segment*
- **Robert LeGrande II**, *Interim Chief Technology Officer, District of Columbia, Office of the Chief Technology Officer (OCTO)*
- **Harlin McEwen**, *Chairman, Communications and Technology Committee of the International Association of Chiefs of Police (IACP)*
- **John Powell**, *Chair, Interoperability Committee and Software Defined Radio Working Group of the National Public Safety Telecommunications Council (NPSTC)*

Session Key Points:

- 700 MHz presents exciting opportunities and proposals, including moving voice channels together, moving data bands together, and the possibility of having a single licensee. This could provide simplicity and the resources to maintain and improve the system.

- Coverage and reliability are critical requirements for public safety wireless broadband systems.

- The National Capitol Region (NCR) is taking advantage of a "perfect storm" of spectrum, money, and technology, leveraging commercial providers, to create interoperable, standards-based broadband systems throughout the region.

- Commercial industry offers a test bed for interoperability, in broadband and voice, and development of new wireless technologies.

- Mr. O'Brien stated that, for the allocation of frequencies in the 700 MHz band, less spectrum is available than would be desirable, but an acceptable outcome from the FCC may be at hand. He added that it's most cost-effective to have spectrum winners, or their partners, who have already deployed networks.

- Different frequency bands (and the distinct, evolving technologies operating in them) are suitable for different uses; e.g., 4.9 GHz is better for incident area networks, 700 MHz for high-speed or jurisdictional area networks.

- CHALLENGES
    - There are multiple, sometimes conflicting needs within public safety.
    - There is a need for networks to be seamless and simple to use: they must work when responders arrive.
    - There is a need for redundancy (and the reliance on LMR) until newer and more complex equipment can meet public safety personnel's need for reliability.
    - There is a need for a business model that provides incentives for commercial interests to partner with public safety, and creation of a governance structure based on consensus and partnerships.

Harlin McEwen, *Chairman, Communications and Technology Committee of the International Association of Chiefs of Police (IACP)*

The public safety community has a couple of opportunities to take advantage of broadband:

- One is in the 4.9 GHz range.
    - We have 50 MHz of spectrum in the 4.9 GHz band, yet it's not intended for mobile applications, but for tactical operations. Many companies are building 4.9 GHz products.
- The big topic, though, is 700 MHz.
    - A year ago, the public safety community's national organizations (IACP, EMS, IAFC, APCO, etc.) were approached by Morgan O'Brien (Cyren Call) about an opportunity to make available new broadband spectrum.

- The FCC on April 25th voted to release Report & Order (R&O) and Notice of Proposed Rulemaking (NPRM) on many 700 MHz issues. It's on a fast track. Comments are due May 23. Reply comments are due seven days later.

Spectrum Chart: One proposal for the public safety 700 MHz spectrum is to move narrowband together (upper) and data (lower) and provide only broadband channels (not wideband). In rural areas, it's too costly for public safety to build the number of cell sites necessary to accommodate broadband. A challenge for public safety is that the FCC proposes one licensee manage all additional spectrum. Public safety has never relied on a single licensee to represent its thousands of agencies.

John Powell*, Chair, Interoperability Committee and Software Defined Radio Working Group of the National Public Safety Telecommunications Council (NPSTC)*

- The Public Safety Wireless Advisory Committee (PSWAC) committee (1996) identified spectrum needs through the year 2010. The PSWAC report identified critical factors for commercial systems before public safety would consider using them. Broadband networks will have to incorporate these before we're going to buy into the networks.

- Coverage of commercial systems is a problem for public safety. Most broadband commercial service doesn't cover areas where public safety needs to be; for example, to be able to fight wildfires in national parks. There's more to consider than whether service is there or not. Several devices use Evolution-Data Optimized (EvDO), which is a candidate technology we want to look at, but we need to look at its technical issues.

- Most public safety voice systems are built to 99.999 percent availability (i.e., less than 5 minutes of downtime a year). This is typical of public safety voice communications systems. We need the same reliability for proposed broadband systems.

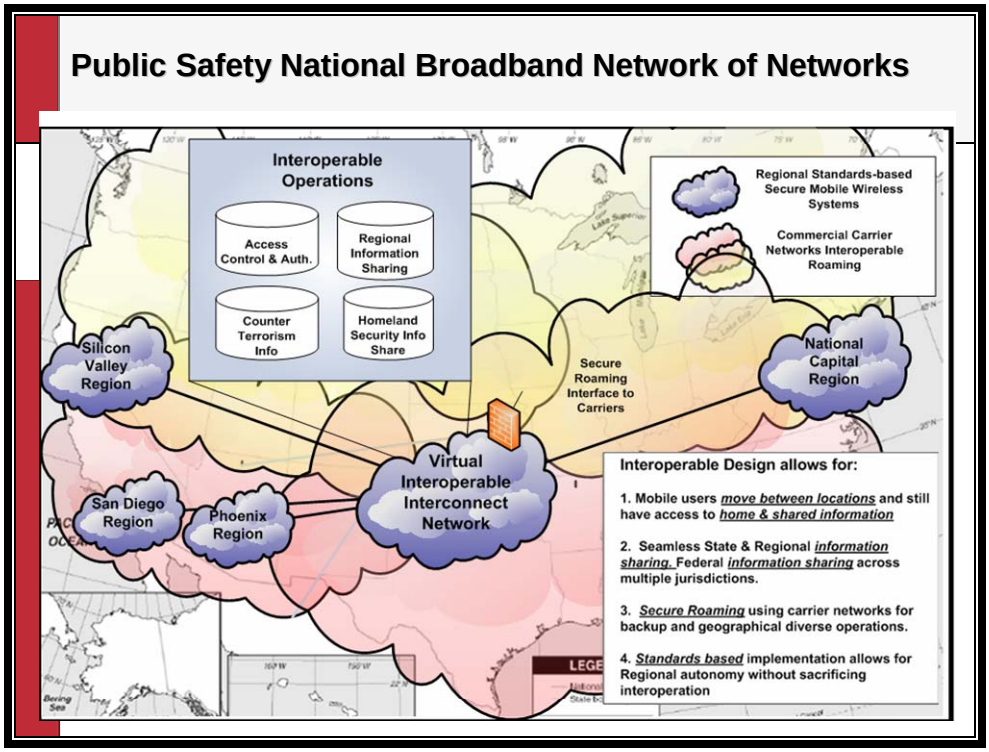
Robert LeGrande II, *Interim Chief Technology Officer, District of Columbia, Office of the Chief Technology Officer (OCTO)*

- The current spectrum and technology situation we have could be considered a "perfect storm." How often is money *and* spectrum available? How often is spectrum available coupled with innovation and mature broadband technologies?

- We were challenged to provide public safety applications—such as Computer Aided Dispatch (CAD), video, and desktop extension—all in a mobile environment. Voice is still a priority, but now there is a migration path and opportunity. We need to consider subscriber devices (data) and LMR migrating to integrated voice/data/video on the same device.

- The initiative started in DC with an operational pilot that has been in operation for the last 2.5 years. We gained experience with deploying and maintaining this broadband system. We took this to our regional partners and asked: what if we all use the same wireless technology, same frequency, and also interconnect fiber networks and address data interoperability? We're working with 19 jurisdictions in the NCR.
    - There are many options out there and the local jurisdictions were considering various different options, which would have caused a problem.
    - We currently have 10 broadband base stations in DC.

- A network of networks is the vision. It's cost-effective and a far more reliable infrastructure. Building this as a public safety grade system will result in a high-powered network.



- Broadband is different than voice from a maintenance standpoint. For example, the user profile is very different. Many applications are active on the network at the same time. The profile of each user becomes very difficult and you must decide who will control access.
    - We should be interoperable with commercial networks. Ideally we'd have several carriers which would create competition.
    - We should also look at all levels of government for interoperability (i.e., state, local, Federal).
    - We should expand our thinking and leverage commercial providers to help fill in the gaps where our networks don't provide service

Comments from Dr. Boyd, *Director, Command, Control and Interoperability, DHS*

- The Federal Government representatives are neutral players. We're not here to endorse or attack any solution.

- This is a "perfect storm." It's an opportunity we're only going to see once. Remember how long it took to get the 700 MHz band freed up? Congress started this reallocation in 1997. None of us will see this again; therefore, the decisions we make over the coming years are going to be crucial.

- It's imperative that we think about how we make this a "system of systems" that brings them together in the way we need. We can't just think about public safety or commercial needs individually. We have to think about both.

- The public safety wireless infrastructure investment is very expensive. Some estimate the value of the systems together would be in the $100B range. We need to determine how to leverage what have and tie it together. For example, public safety has used commercial access for a long time. What is the best approach for this relationship?
    - Make sure industry understands what public safety needs at the operating level.
    - At the end of the day, it has to do with citizens' lives.
    - We need you to get together to develop a solution to serve the Nation.

Comments from Industry Representatives

Christopher Guttman-McCabe, *Vice President, Regulatory Affairs, CTIA*

- We all believe interoperability will happen. A question is, will it be a slow change or a significant change?

- There is a test bed: the commercial industry. The commercial industry will allow us to see what's possible. Interoperability exists in commercial industry across multiple providers. We all agree there is a great difference in application when you talk about public safety.

- The NCR is providing another test bed in the broadband space. Is it possible in the voice space? Look at opportunities out there: voice, video, digital imaging, database access all together.
    - These applications can happen much faster on commercial broadband devices. This is the first time public safety is considering how it can take advantage of what's in the commercial space.
    - There's competition, redundancy, and the ability to ride on a dedicated network and roam to commercial network. There's the ability to grab onto the coat tails of commercial industry.

- Currently High Speed Downlink Packet Access (HSDPA) and other broadband services are available (Verizon, Sprint – EvDO Rev. A). We have second-generation cellular data services (2G), have moved to 3G, and standards bodies are working on 4G. This evolution is happening. Standards organizations are discussing how to support public safety's needs. There is an opportunity to leverage what's happening in the commercial arena and take advantage of its economies of scale, etc.

Morgan O'Brien, *Co-founder and Chairman, Cyren Call Communications*

- We filed an application over a year ago with the intent to create a clamor—a sense of urgency—and to suggest a solution. We were successful in creating a clamor. We're moving out of the conflict phase and are on the verge of resolution.

- We're approaching with a process aimed at feeding the FCC useful opinions.

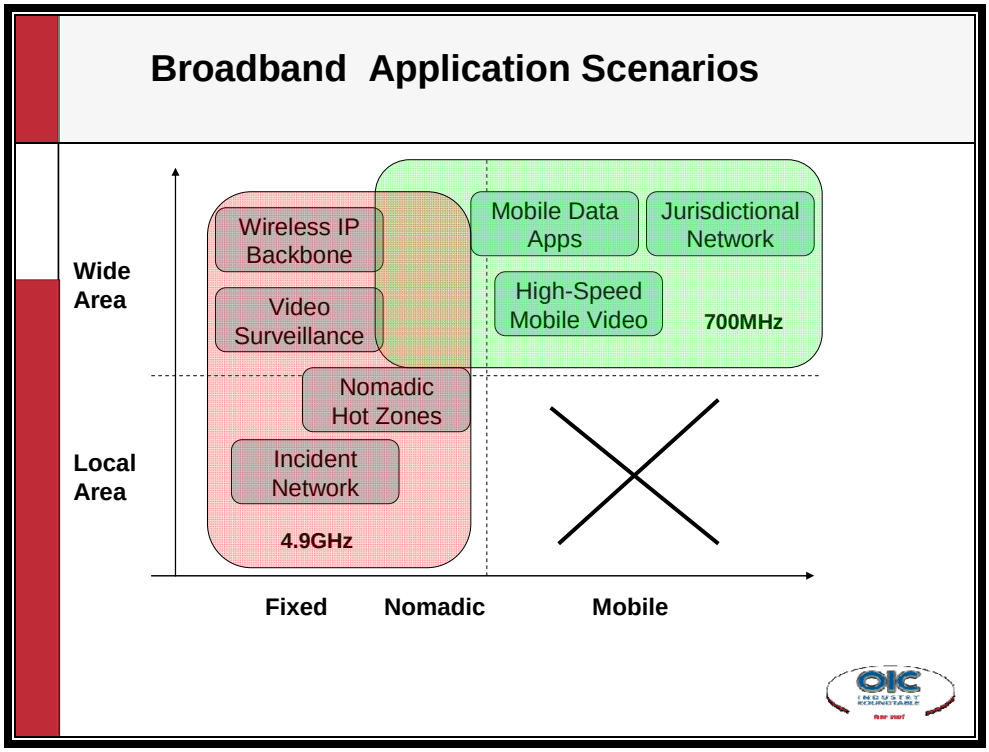
- Our attention is on trying to figure out how to make the auction process work for public safety.

- There is now less spectrum being considered; Cyren Call thought 30 MHz was the minimum. With less spectrum, it becomes more important to make sure we find the right

partner for public safety (i.e., the winner of the auction) and that FCC service rules encourage the right partner.
    - When working with less spectrum, it's advantageous if a partner has a deployed network: this can cut percentages from capital expenditures needed to start a network and reduce the time to deploy.

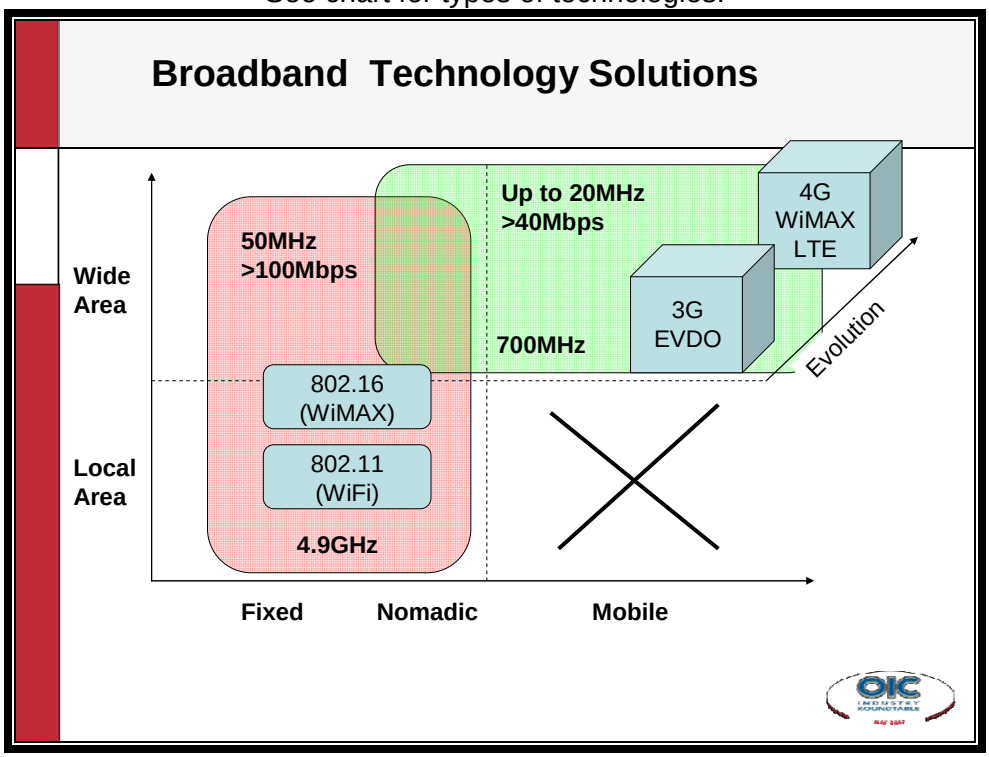
Greg Henderson, *Manager of Broadband Technology, Tyco Electronics Wireless Systems Segment*

- Broadband consists of a variety of applications—local and wide-area, fixed, nomadic, and mobile networks.



- Many fixed, wide-area solutions are being deployed (for example, video surveillance is popular). However, there is a great need to move broadband applications toward supporting full mobility.
    - This is the Jurisdictional Area Network (JAN) concept—a concept that would support high-speed mobile video. There is no one technology or solution to fit this area. Possible Solutions are in 4.9 GHz and 700 MHz bands.

See chart for types of technologies.



- The 4.9 GHz band has 50 MHz of spectrum dedicated to public safety.
    - There are solutions using two major technologies in this band—802.11 WiFi, and 802.16 WiMax.

- There will be somewhere around 20 MHz allocated in the 700 MHz band if not auctioned. This spectrum supports speeds above 40 megabits per second (Mbps).
    - This provides an opportunity for wider area mobile broadband.
    - It's important to evaluate 4G technologies which are defined as a flat Internet protocol (IP) network, using 5 MHz wide channels or wider.

Questions from Dr. Boyd

How do we do it best? How does public safety sign on to making these things happen? How do we implement broadband and make it widely available?

John Powell: One major obstacle is that there is not agreement between public safety across the thousands of agencies across the Nation. Many take different positions with the FCC, etc. There's metropolitan vs. rural, for example. In regards to the 700 MHz allocation, there's the issue of one licensee vs. each agency holding its own license.

- Whatever technology we choose, we need a method to bring broadband subscriber devices with us on an incident to self-form a network and operate without backhaul.

Robert LeGrande II: Officials from Federal, state, and local governments are all looking at different technologies and different frequencies. Therefore, if we're not careful, we may end up exactly where we are today, with an approach that is not unified.

- We must look across the country in order to support mutual aid. If we don't work together, we run the risk of hampering interoperability.

Harlin McEwen: We need high-level decisions in a short period of time. The FCC is clear that the 700 MHz issue is fast moving; although we've spent the last 10 years dealing with it, the time for decision is now. At the national level, key national executive organizations (the International Association of Chiefs of Police (IACP), the International Association of Fire Chiefs (IAFC), the National Sheriff's Association (NSA), the Association of Public-Safety Communications Officials (APCO), the National Association of State EMS Officials (NASEMSO), etc.) have been meeting daily for the last two weeks to develop a consensus position to file (probably through NPSTC) on behalf on organizations.

- We must develop a consensus filing and tell the FCC what's critical to public safety. The most critical issue in our discussions is to point out that this proposed network is different than a commercial network.
- We're talking about a partnership, not building a commercial network. An issue for us is: how do we control the destiny, needs, and important interest of public safety? We don't want to give up control of things like reliability, security, redundancy, etc. If we don't address this, we haven't done our job.

Breakout Recommendations (from audience members):
Question: What should OIC do, and what should we be aware of going forward?

- None of these solutions are perfect; it's important to pick one and make it work.
- Broadband communication capabilities are needed now.
- Public safety needs to be aware that its legacy systems will still need to be maintained, or even upgraded, while paying having to pay additional usage fees for a broadband system. This presents funding problems.
- Develop approaches for risk mitigation.
- Carriers ought to tell the FCC that more time is needed to handle issues of this complexity (despite the statutory deadlines).
- Focus on governance, and incorporate interests of public safety.

Broadband Q&A:

Q Do you look at DHS to lead the charge for public safety and, if so, how?
A *McEwen*: At this point, DHS doesn't have much of a role. It's a state and local matter for the FCC to choose how we're going to move forward. We have a DHS partnership to leverage tools which enters into our decision making. DHS provides opportunities to bring people together as it's doing at this conference. DHS will play into our decisions, but it's primarily a local public safety decision.

Q When we go with more bandwidth, don't we need special characteristics on the transmit side (e.g., more power) and won't we need huge subscriber devices to pull this off? What is the technology necessary for broadband?

A *LeGrande II:* The vast majority of public safety today relies on commercial data networks. We're doing it for automatic vehicle location and using cellular data transmission technologies like 1xRTT, Cellular Digital Packet Data (CDPD), and now EvDO. It's widely available because it took so long for us to get our spectrum. Industry (Alcatel, Lucent, Qualcomm, etc.) have shown us subscriber devices that could meet our needs. We've already operated a broadband network in Washington, D.C. and used, for example, laptops with a wireless PC card. Once the 700 MHz spectrum opens up, many new devices will be made available.

A *McEwen:* We're not planning on abandoning mission-critical LMR voice systems for a long time; not until broadband wireless is reliable and we're comfortable with it. However, with regard to broadband data, the networks aren't as widespread as they need to be given the great need.

A *Powell:* The San Diego police are making use of broadband and catching a lot of criminals every day using their wireless data technology. Redundancy doesn't mean more of a complex system. We need to be cautious moving away from traditional LMR to broadband until there is sufficient capability.

A *Guttman-McCabe:* We talked about the evolution of broadband in CTIA's meeting on broadband, but recognized that legacy systems will be in place for a long time. Will there be a single nationwide licensee and a single technology? EvDO may be a legacy system by the time this happens.

A *LeGrande II:* One of the benefits of a single public safety licensee is that the operator will have access to resources to deal with issues that others bring up. It's a complex undertaking to layer a new next-generation technology into this existing public safety life and death environment. This is simplified with a single licensee combined with adequate funding.

Q What does the governance structure look like?

A *Guttman-McCabe:* I like the idea suggested by Morgan. If we want to dedicate 10 MHz to a partner/commercial operator, then there must be incentive for the commercial operator to participate. One proposal contains "poison pills" (i.e., disincentives) which will need to be reduced or eliminated.

A *Henderson:* An issue raised is public safety experience with commercial technology. It's assumed that if the system is not 100 percent available, it's not appropriate. The goals are cost and capacity. This depends on how the network is deployed. Most believe that technology can meet public safety requirements if deployed properly. The question is: how?

A *LeGrande II:* The NCR believes that regions can build out private networks, but we should agree on frequency and technology. We can make private networks cost effective. Locals lead efforts in our governance program and legislators have the ultimate decision on applications, access, major changes, and operational changes. We believe this puts us in a good position to partner with national organizations to ensure interoperability with national networks.

A *McEwen:* I think that's an important issue. Under a national license concept, how much of the spectrum should be held in reserve for operation of local systems? We agree that some portion should be reserved for this purpose. The FCC feels that none should be reserved and all should be under a national licensee. The question is: how much?

A *Powell:* In recent comments and in his speech yesterday, Chertoff said technology is not the issue, it is governance. It's a matter of building consensus and building partnerships with the public safety community and commercial providers and putting aside their own interests for the good of a national solution.

Q Morgan, is it fair to say that you are giving up on pursuing a petition to the FCC?

A *O'Brien:* For the moment, the FCC has taken charge of this process in a way that could end up in a real workable solution that's not as good as that which we first proposed, but one that's acceptable and achievable. If the FCC decides to go with a regular auction, we would address this with Capitol Hill. I predict that an acceptable outcome will be crafted out of this process.

A *Dr. Boyd:* We need to do something to strengthen communications. There are many alternatives; the challenge is to reach consensus and build something viable and useful for public safety.

Closing Remarks

Dr. David Boyd
Director of the Department of Homeland Security's Office for Interoperability and Compatibility (OIC)

- As I had hoped, this has been an incredibly productive event with several significant outcomes resulting from our efforts together.
    - We have heard first-hand accounts of emergency responders in the field—once again highlighting the critical need for technological advances in communications interoperability.
    - We have challenged you to formulate strategies and solutions to these critical technology issues and we have received strong responses to this challenge.
    - We have discussed the FY 2007 interoperable communications grant programs and clarified issues among the group.
    - We have shared thoughts regarding the value of current emergency interoperable standards efforts, while exploring the possibilities that may result from their adoption and implementation.
- I hope you have found the Roundtable as valuable as I have. On a personal note, I have enjoyed meeting with many of you and hearing firsthand your suggestions and recommendations in support of improving interoperable communications.
- Members of OIC's Federal leadership team look forward to seeing you at the Science and Technology Directorate's Stakeholders Conference on May 21-24 at the Ronald Reagan Building and International Trade Center here in Washington, DC.
    - One of the breakout sessions at this conference will focus on the Roundtable—including outcomes and next steps.
- We recognize the critical role of our industry partners in OIC's critical national mission—and we thank you for your continued efforts.

Appendix: Presenter Bios

Major Speakers

Dr. David Boyd
Director of the Office for Interoperability and Compatibility, DHS

Dr. David Boyd joined DHS in March 2003 and serves as the Director of the Command, Control and Interoperability Division within the Science and Technology Directorate. In this role, Dr. Boyd is responsible for research and development programs to support command and control, communications, computing, intelligence, surveillance, and reconnaissance. He is also the Director of OIC. Before joining DHS, Dr. Boyd served as the Director of Science and Technology for the National Institute of Justice. He has served on the White House National Science and Technology Council, the National Security Council Committee on Safety and Security of Public Facilities, and as the Executive Chair of the Department of Justice's Technology Policy Council. Dr. Boyd retired from the U.S. Army after more than 20 years to enter the Civil Service. His more than three dozen military awards including the Bronze Star and the Purple Heart. He is a recipient of a 2005 Presidential Rank Award, the highest recognition available in the Federal Civil Service. He holds a career appointment in the Senior Executive Service, and is a graduate of the University of Illinois–Champaign, Golden Gate University, the University of Illinois–Chicago, and Walden University. Dr. Boyd holds graduate degrees in Operations Research and Public Policy Analysis, and a doctorate in Decision Sciences. He has published extensively in military, law enforcement, technical, and general-circulation publications.

Secretary Michael Chertoff
Secretary of DHS

On February 15, 2005, Judge Michael Chertoff was sworn in as the second Secretary of DHS. He formerly served as United States Circuit Judge for the Third Circuit Court of Appeals. Secretary Chertoff was previously confirmed by the Senate to serve in the Bush Administration as Assistant Attorney General for the Criminal Division at the Department of Justice. As Assistant Attorney General, he helped trace the 9/11 terrorist attacks to the al-Qaeda network, and worked to increase information sharing within the FBI and with state and local officials.

Before joining the Bush Administration, Secretary Chertoff was a Partner in the law firm of Latham & Watkins. From 1994 to 1996, he served as Special Counsel for the U.S. Senate Whitewater Committee. Prior to that, Secretary Chertoff spent more than a decade as a Federal prosecutor, including service as U.S. Attorney for the District of New Jersey, First Assistant U.S. Attorney for the District of New Jersey, and Assistant U.S. Attorney for the Southern District of New York. As United States Attorney, he investigated and prosecuted several significant cases of political corruption, organized crime, and corporate fraud.

Secretary Chertoff graduated magna cum laude from Harvard College in 1975 and magna cum laude from Harvard Law School in 1978. From 1979-1980 he served as a clerk to Supreme Court Justice William Brennan, Jr.

Under Secretary Jay Cohen
Under Secretary for Science and Technology, DHS

(In addition to participating in the opening session, Under Secretary Cohen delivered remarks on behalf of Secretary Michael Chertoff at the luncheon on Wednesday, May 9, 2007.)

Under Secretary for Science and Technology at the Department of Homeland Security, Jay M. Cohen is a native of New York. He was commissioned in 1968 as an ensign upon graduation from the United States Naval Academy. He holds a joint Ocean Engineering degree from Massachusetts Institute of Technology and Woods Hole Oceanographic Institution, and Master of Science in Marine Engineering and Naval Architecture from MIT. His early Navy assignments included service on conventional and nuclear submarines. From 1985 to 1988 Cohen commanded USS HYMAN G. RICKOVER (SSN 709). Following command, he served on the U.S. Atlantic Fleet as a senior member of the Nuclear Propulsion Examining Board, responsible for certifying the safe operation of nuclear-powered ships and crews. From 1991 to 1993, he commanded USS L.Y. SPEAR (AS 36) including a deployment to the Persian Gulf in support of Operation DESERT STORM. Cohen was promoted to the rank of Rear Admiral in October 1997 and reported to the Joint Staff as Deputy Director for Operations responsible to the President and DoD leaders for strategic weapons release authority. In June 1999, he assumed duties as Director Navy Y2K Project Office responsible for transitioning all Navy computer systems into the new century. In June 2000, Cohen was promoted in rank and became the 20th Chief of Naval Research. He served during war-time as the Department of the Navy Chief Technology Officer (a direct report to the Secretary of the Navy, Chief of Naval Operations and Commandant of the Marine Corps). Responsible for the Navy and Marine Corps Science and Technology (S&T) Program (involving basic research to applied technology portfolios and contracting), Cohen coordinated investments with other U.S. and international S&T providers to rapidly meet war fighter combat needs. After an unprecedented five and a half year assignment as Chief of Naval Research, Rear Admiral Cohen retired on February 1, 2006. Under Secretary Cohen was sworn in to his current position at DHS on August 10, 2006.

Assistant Secretary Greg Garcia
Assistant Secretary for Cyber Security and Communications, DHS

Gregory T. (Greg) Garcia was appointed by Secretary Michael Chertoff on September 18, 2006, to be America's first Assistant Secretary for Cyber Security and Telecommunications (CS&T) for the Department of Homeland Security, within the Preparedness Directorate. Mr. Garcia is responsible for the National Cyber Security Division, which works collaboratively with public, private, and international entities to secure cyberspace and America's cyber assets, and for the National Communications System, which coordinates and plans for national security and emergency preparedness communications for the federal government.

Prior to joining the Department, Mr. Garcia served as Vice President for Information Security Programs and Policy with the Information Technology Association of America (ITAA). In this capacity, he managed all programmatic and public policy aspects of information security, with a view to strengthening our national cyber readiness among the user and vendor communities. Additionally, he worked with the Department of Homeland Security to co-found the National Cyber Security Partnership.

Before joining ITAA in April 2003, Mr. Garcia served on the staff of the House Science Committee where he was responsible for industry outreach and legislative issues related to information technology and cyber security. In particular, Mr. Garcia played an active role under the leadership of Chairman Sherwood Boehlert (R-NY) in the drafting and shepherding of the Cyber Security R&D Act of 2002.

Prior to his experience on Capital Hill, Mr. Garcia worked for several organizations on policy issues. He served as Director of 3Com Corporation's Government Relations Office in Washington, DC where he was responsible for all aspects of the company's strategic public policy formulation and advocacy. He also served as Coalition Manager for Americans for Computer Privacy, a high profile grassroots policy advocacy campaign dedicated to overturning U.S. export and domestic use regulation of encryption technology. This effort was successful after just one year of intense lobbying and high-end media strategies.

Mr. Garcia lobbied international trade policy for the American Electronics Association, including export controls, customs, European and multilateral trade negotiations. He also worked for Newmyer Associates, Inc. a public policy consulting firm where he reported and consulted on international trade policy for Fortune 500 clients. Mr. Garcia is a graduate of San Jose State University in California.

Congressman Dave Reichert
Representative from the Eighth Congressional District of Washington
Homeland Security, Transportation and Infrastructure, and Science and Technology Committee Member

Congressman Dave Reichert brings over 30 years of public service experience to Washington. Now in his second term, he serves as the Representative from the Eighth Congressional District of Washington. Congressman Reichert serves on three committees, Homeland Security, Transportation and Infrastructure, and Science and Technology. He has a leadership role in the Committee on Homeland Security, and serves as the Ranking Member of the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment.

During his first term in Congress, Congressman Reichert was only the sixth freshman in the history of the House of Representatives to be given a committee chairmanship. He was appointed Chairman of the Subcommittee on Emergency Preparedness, Science and Technology. In this position, Chairman Reichert led the way in drafting comprehensive legislation to fix the emergency response problems associated with FEMA following Hurricanes Katrina and Rita. This legislation included a section on improving the ability of first responders to communicate during emergencies and it was signed into law on October 4, 2006.

The subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment has jurisdiction over Federal, state, and local intelligence and information sharing efforts within the United States; terrorism-related threat, vulnerability, and risk analyses at DHS; terrorism threat advisories and warnings; Homeland Security Advisory System; liaison of the Department with U.S. intelligence and law enforcement agencies; the role of terrorism threat prioritization; Federal Law Enforcement Training Center (FLETC); Secret Service; and over-classification issues. Congressman Reichert also serves on the Subcommittee on Border, Maritime, and Global Counterterrorism.

From 1971 through 1976, Congressman Reichert was a member of the U.S. Air Force Reserve and in 1976 he was active duty in the Air Force. In 1972 he joined the Sheriff's Office and in 1997 he became King County's first elected sheriff in over 30 years. Under his leadership, the county saw a significant drop in violent crime. Sheriff Reichert brought national recognition to the Sheriff's Office as head of the task force solving the largest serial murder case in U.S. history. As sheriff, he also brought an unprecedented $28 million in Federal funding to King County law enforcement efforts.

Sheriff Reichert is established as a leading voice against domestic violence and an advocate of strong family values. In 2004 Reichert received the prestigious National Sheriffs' Association's "Sheriff of the Year" award. He is a two-time Medal of Valor Award recipient from the King County Sheriff's Office and was honored with the Washington Policy Center's Champion of Freedom Award. Reichert received the Families Northwest Public Policy Award and took top honors in a local television network's (King 5) leadership poll.

Sheriff Reichert was president of the Washington State Sheriffs' Association and an executive board member of the Washington Association of Sheriffs and Police Chiefs. He has served on numerous advisory boards including the King County Criminal Justice Council and the King County Domestic Violence Council. He co-chaired the Washington State Partners in Crisis, a statewide coalition targeting issues related to mental health.

Representative Bennie Thompson
Democratic Congressman from Mississippi's Second District
Chairman, Homeland Security Committee

Bennie G. Thompson is now serving his eighth term as the Democratic Congressman from Mississippi's Second District and third term on the Homeland Security Committee. The Second District stretches from Tunica in the north to Jefferson County in the south and all points in between, creating a rare blend of agricultural economies and the hustle and bustle of city life.

Congressman Thompson has spent his entire adult life giving a voice to the voiceless. With 39 years of continuous public service, he is the longest-serving African-American elected official in the state of Mississippi. His reputation as a no-nonsense problem solver has earned him the trust of his constituents and the respect of his colleagues in Washington. In 2000, Congressman Thompson's legislation creating the National Center for Minority Health and Health Care Disparities became law. Long considered a leading voice on civil rights, equal education, and healthcare reform, Congressman Thompson has helped to make a real difference in the lives of his constituents. In 1975, he filed a lawsuit to increase funding at Mississippi's historically black universities. With Congressman Thompson as lead plaintiff, the case was settled in 2004 for an unprecedented $503 million.

Congressman Thompson served on the Agriculture, Budget and Small Business Committees before assuming the top Democratic position on Homeland Security in 2005. During his tenure as Ranking Member of the Homeland Security Committee, Congressman Thompson secured millions of dollars in post-Katrina contracts for small and minority businesses in Mississippi to assist in the rebuilding efforts of the ravaged Gulf Coast. In addition, after experiencing first hand FEMA's failure in handling the response to Hurricanes Katrina and Rita, Congressman Thompson became the driving force behind the restructuring of the broken agency. In conjunction with the Senate, Congressman Thompson successfully created a new and

improved FEMA, one with the ability to respond quickly and effectively to any terrorist attack or natural disaster.

Drawing on his 26 years of experience as a volunteer firefighter in Hinds County, Congressman Thompson understands that our nation's law enforcement and first responders are our first line of defense in times of emergency. With that in mind, he has constantly fought to ensure they are fully equipped with the resources and tools they need to effectively respond to any and all emergencies. After successfully serving as Ranking Member for the past two years, his colleagues promoted Congressman Thompson to serve as the first ever Democratic Chairman of the Homeland Security Committee.

Born in Bolton, he attended Hinds County public schools before earning degrees from Tougaloo College and Jackson State University. After serving as alderman and mayor in his hometown for 12 years, Congressman Thompson served as Hinds County Supervisor for 13 years before being elected to Congress in 1993.

Colonel Victoria A. Velez
Director of the Office of Emergency Communications
Department of Homeland Security

Colonel Victoria A. Velez is the Acting Director of the Office of Emergency Communications within DHS. Colonel Velez's career path includes multiple commands and staff positions which have provided direct and tangible impacts to the Joint Warfighter. Most recently, she served as Commander of the Joint Interoperability Test Command in Fort Huachuca, Arizona and Chief of Staff for the National Communications System of DHS. Among her many assignments, Colonel Velez has supported operations including Desert Thunder, Desert Storm, Noble Anvil/Allied Force, Enduring Freedom, and Iraqi Freedom. Her decorations include Defense Meritorious Service medal (one oak leaf cluster), the Meritorious Service Medal (three oak leaf clusters), the Air Force Commendation Medal, and the Joint Outstanding Unit Medal (CENTCOM, one oak leaf cluster), and she was named one of *Government Computer News'* Ten Outstanding DOD leaders for 2003. Colonel Velez was commissioned a second lieutenant in the United States Air Force through the Reserve Officer Training Corps at the University of Maryland upon her graduation with a Bachelor of Arts degree in June 1981. She also earned a Masters of Arts Degree from Webster University in 1987. Her military education includes Squadron Officer's School, Advanced Communications Officer Training, Air Command and Staff College (ACSC), and the Air War College.

A View from the Front: The Emergency Response Experience

Brian Fennessy
Battalion Chief and Director of Air Operations, San Diego Fire-Rescue Department

Chief Brian Fennessy began his Fire Service career in 1977, and has 31 years of experience in fire suppression, rescue, and the emergency medical field. During his first 14 years in the fire service, he worked for both the United States Forest Service (USFS) and the United States Bureau of Land Management (BLM) and was stationed primarily in Southern California. As a firefighter, Chief Fennessy traveled throughout the United States, including Alaska, battling wildfires from the air and ground. While with these two agencies, he led, managed, and supervised hotshot crews, engine crews, and helicopter crews. In 1987, he was instrumental in developing and implementing the BLM's first medium-lift helicopter and heli-rappel program.

In 1990, Chief Fennessy was hired by the City of San Diego Fire-Rescue Department. As a result of his previous and current employment, he maintains multiple Incident Command System (ICS) qualifications and currently serves as an Air Operations Branch Director (AOBD) on a Federal Incident Management Team. Each year, this team is dispatched throughout the United States to manage large fires and "all hazard" incidents.

In 1997, Chief Fennessy began developing the concept of a regional fire and rescue helicopter program that would enhance emergency service delivery to better serve the citizens and visitors of San Diego County. At the time, the region was the only large Southern California County not served by year-round, medium-lift, aerial firefighting and rescue helicopters. From 2000 to 2002, the program successfully implemented short-term programs and during that period, operated a Bell 407, a Bell 206 L4, and a Bell 212HP helicopter. In 2003, the San Diego Fire-Rescue Department Air Operations Division began year-round operations with a Bell 212HP helicopter and in 2004, added a Bell 205A1++ helicopter. In addition to day and night (NVG) aerial firefighting operations, the Division introduced day and night (NVG) hoist rescue and EMS operations to the region, and frequently provides air medical transportation to the injured. In February 2007, the Division began operating and responding on a 24-hour basis and is currently one of only three fire departments in California providing round-the-clock, full-service, multi-mission emergency helicopter services. In May 2005, Chief Fennessy was promoted to Battalion Chief and continues to lead, administer, and direct the Department's cutting-edge Air Operations Division. Chief Fennessy also represents the SDFD on multiple committees pertaining to fire and aviation operations.

Chief Fennessy is recognized in the United States as an expert in the aerial firefighting and air rescue field. He is an instructor for wildland firefighting and rescue courses; he provides air rescue training, hoist rescue operations training, and other aviation-related training. He has also provided formal air operations training at training courses and workshops on a national, state, and local level. Because of his knowledge and many years of experience in the aerial fire, rescue, and EMS field, Chief Fennessy is often recruited to speak and make presentations to the fire and aviation community about these experiences.

Eric Mello
Chief, Westerly Police Department

Edward Mello was appointed to the position of Chief of Police of the Westerly Police Department in August of 2005. The department is served by more than 75 full-time staff and 35

part-time staff, serving a resort community with a population of approximately 30,000 people. The summer population swells to more than 60,000.

Chief Mello was born and raised in Westerly and attended the public school system and went on to receive his Bachelors degree in Criminal Justice from Roger Williams University. He is currently pursing his graduate degree from Boston University. In addition, to numerous law enforcement training programs in both the area of operations and administration, Chief Mello is a graduate of the FBI National Academy.

Beginning as a patrol officer in 1988, the Chief was promoted to the rank of patrol sergeant in 2001. He was then promoted to the rank of captain in 2002. During his service to the department, Chief Mello has been responsible for patrol operations, investigative services, and the general administration of the department with an annual operating budget of more than $4 million.

For nearly five years, Chief Mello has spearheaded the project to build a new 31,000-square-foot police headquarters at a cost of more than $12 million. The state-of-the-art facility is expected to open in the fall of 2007, replacing the existing 1950-era headquarters.

Mike Todorovich
Interoperable Communications Coordinator, West Virginia Department of Military Affairs & Public Safety

Mike Todorovich started working for the West Virginia Department of Military Affairs & Public Safety within the Office of the Secretary of the Homeland Security State Administrative Agency (HS SAA) in February 2007. As Interoperability Coordinator, his primary responsibility is to plan, coordinate, and guide processes for continued development of a statewide connectivity and interoperability system which is generic (transparent) to the various types of systems with local, state, and Federal agencies. He will also serve as primary communications advisor to Cabinet Secretary Jim Spears, and to Mr. Terry Miller, Director of the HS SAA.

Mr. Todorovich received his Bachelor's degree from University of Charleston, and a Masters of Religion from Liberty University. With forty years of service, he recently retired—at the rank of Lieutenant Colonel—from the West Virginia Army National Guard. During his military service, Mr. Todorovich served the last 22 years as a Federal technician as J6 and Deputy Chief of Staff, Information Management (DCSIM). In this position, he led information technology efforts, including automation, telecommunications, information technology security, interoperability initiatives, and visual information for over 50 physical sites and 2,000 users.

Mr. Todorovich has earned many awards and accolades during his career, including the Legion of Merit, Order of St. George Armor Award, and the Meritorious Service Award, among others. He served as the Past President of the West Virginia Officer's Association and the Past President of the West Virginia National Officer Candidate School Alumni Association. He considers it an honor and privilege to serve his nation and state as Interoperability Coordinator.

Breakout Series I: Session A: Grant Guidance: What You Need to Know

Tony Frater
Deputy Director
Office for Interoperability and Compatibility, DHS

Over the past nine years, Tony Frater has worked in government and the private sector promoting the use of technologies to improve interactions among local, state, and Federal governments. Before joining the DHS Command, Control and Interoperability division as the Deputy Director of OIC, Mr. Frater was a Vice President at Dutko Worldwide and was the firm's primary interface to clients for technology and budget-related issues. In this role, he worked with clients to build coalitions and formulate strategies to establish public-private partnerships. Mr. Frater's clients included state and local governments, non-government organizations, and private sector companies. Prior to joining Dutko Worldwide, Mr. Frater worked at the White House Office of Management & Budget (OMB) where he specialized in information technology (IT) issues. As the Government to Government (G2G) Portfolio Manager, he was responsible for implementing the "Expanding E-Government" initiative of the President's Management Agenda. In this position, he led an extensive change management effort to harmonize business processes and interactions among Federal, state, and local governments within five key programs: Interoperable Communications, Disaster Management, Grants Management, Exchange of Vital Statistics, and Geospatial Information Management. At OMB, Mr. Frater also served as a Policy Analyst in the Information Policy & Technology Branch. He developed and recommended strategies to improve the value and effectiveness of IT systems and technology program operations for the Executive Branch. He also developed and implemented IT management policies including revisions to OMB Circular A-130 "Management of Federal Information Resources" and OMB Circular A-16 "Coordination of Geographic Information, and Related Spatial Data Activities." Mr. Frater has a joint Master's degree in Public Administration and Information Science from the University of Pittsburgh and a B.A. in Political Science from the University of Minnesota.

Scott Kelberg
Director, Technical Assistance Division, Capabilities Division
Federal Emergency Management Agency, DHS

Scott Kelberg is the Director for the Technical Assistance Division within the Capabilities Division (CD), National Preparedness Directorate, Federal Emergency Management Agency, Department of Homeland Security (DHS). Mr. Kelberg supervises program and policy development, including the FY07 Homeland Security Grant Program and Buffer Zone Protection Program; development and delivery of technical assistance programs; and information collection and analysis. Prior to being assigned this responsibility, Mr. Kelberg was the Branch Chief within the Special Projects and Policy Development Branch within CD. He was responsible for programmatic and fiscal oversight, planning, development, and assessment of grant assistance programs and cooperative agreements. These provide funding for training and technical assistance to state and local emergency responders and public safety officials to address weapons of mass destruction response planning and emergency preparedness. He was also responsible for the management and oversight of the National Domestic Preparedness Consortium (NDPC) training programs. Mr. Kelberg previously worked at the Department of Justice, Bureau of Justice Assistance, working on law enforcement intelligence systems. In addition, he has also worked for the Montgomery County Department of Corrections. Mr.

Kelberg received a Bachelor of Arts degree in Political Science from Syracuse University and a Master of Science in Justice Law and Society from American University. He is a native of Philadelphia.

Laura M. Pettus
National Telecommunications and Information Administration
Department of Commerce

Laura Pettus joined the National Telecommunications and Information Administration in February 2007 and serves as the Communications Program Specialist for the Public Safety Interoperability Communications (PSIC) Grant Program. In this role, Mrs. Pettus provides guidance and assistance to the Assistant Secretary and senior NTIA officials in the formulation, development, and implementation of the $1 billion PSIC Grant Program to enhance interoperable communications capabilities for public safety agencies. Prior to joining NTIA, Mrs. Pettus served as the citywide Grants Coordinator for the City of Alexandria, Virginia where she worked with over 20 local agencies in the management of state and Federal grants. As Grants Coordinator, Mrs. Pettus was responsible for the management of the city's critical interagency grants dealing with homeland security, law enforcement, and disaster assistance. Mrs. Pettus began her work with the City as an Emergency Management Analyst for the Alexandria Fire Department. Her professional experience also includes service as the Director of Operations for a start-up pharmaceutical company and service as an economic research analyst for the Alliance to Save Energy. Prior to arriving in the Washington, DC, area, Mrs. Pettus worked in the Office of the Head Economist in St. Petersburg, Russia, to assist with balancing the city's first budget in the aftermath of the devaluation of the Russian ruble. Mrs. Pettus received a B.A. in Economics with Honors from Kenyon College and resides in Alexandria, Virginia.

Breakout Series I: Session B:
Emergency Interoperable Data and Messaging Standards Efforts

Mike Daconta
Vice President, Enterprise Data Management, Oberon Associates, Inc.

Mike Daconta is the Vice President of Enterprise Data Management for Oberon Associates, Inc., where he is currently leading several data management projects for customers including the Transportation Security Administration, or TSA. He is a well-known author, lecturer, and columnist, having authored or co-authored 10 technical books, numerous magazine articles, and online columns. Previously, Mr. Daconta was the Metadata Program Manager for DHS where he spearheaded data standardization, stewardship, and metadata registration. He was selected by the Office of Management and Budget and the Federal CIO Council to lead the Federal Enterprise Architecture (FEA) Data Reference Model (DRM) Working Group which successfully delivered DRM V2.0 in December 2005. In conjunction with the Department of Justice he launched the National Information Exchange Model (NIEM) to provide a reusable set of core XML components for building exchange packages. Other past assignments include the Chief Architect of the Defense Intelligence Agency's Virtual Knowledge Base Project and designer of the electronic mortgage XML standard for Fannie Mae. His most recent book is entitled, *The Semantic Web: A Guide to the Future of XML, Web Services and Knowledge Management*. His other books cover XML, XUL, Java, C++ and C. He earned his Masters

degree in Computer Science from Nova Southeastern University and his Bachelor's degree in Computer Science from New York University.

Theresa Lynn Hadden
Senior Applications/Information Architect, Fairfax County, Virginia

Lynn Hadden is a Senior Application/Information Architect for Fairfax County, Virginia. Prior to this position, she has served as a teacher, a programmer, an application consultant, a senior software engineer, a Project Manager, and an Internet Architect. She received her BS in Finance from Louisiana State University in 1983 and her MBA in 1985. As an applications consultant in the Office of Computing Services at Louisiana State University Ms. Hadden designed, developed, and managed the LSU Digital Library Project and the LSU Electronic Reserve System. As a Senior Software Engineer for Signal Corporation, Ms. Hadden participated in the design and development of the General Services Administration's Tracking and Ordering System. She accepted her position with Fairfax County as an Internet Architect for the Library in 1999. She moved into the Department of Information Technology in the year 2000. Her main job responsibility is implementing an information/application architecture for the county that will allow for interoperability across and among internal and external information systems. In addition to her Fairfax County internal work, she has been asked by the county's CTO to lead a regional Interoperability Initiative: the NCR Data Exchange Hub. This particular project relies heavily on her experience with integration and interoperability. This project will deliver a real-time interactive system designed to strengthen the flow of information between emergency support functions such as Fire Response, Law Enforcement, Emergency Management, Mass Care, Health, and Communication, and Transportation within the National Capital Region (NCR). This system will provide communication, collaboration, and information exchange capabilities to all 19 jurisdictions within the NCR, facilitating faster and better response to an emergency.

Chip Hines
Program Manager, Disaster Management e-Gov Initiative, DHS

Chip Hines has over 30 years of experience working in the emergency management field, with more than 15 of these spent developing and managing Federal programs and systems designed to assist the United States government in being better prepared to manage emergencies. He has worked in the areas of National Preparedness, Emergency Operations, and State and Local Preparedness, as well as in Preparedness, Training, and Exercises at the Federal level. Mr. Hines is the Program Manager for the Disaster Management e-Gov Initiative, run out of the Science and Technology Directorate, a directorate within DHS. He holds a Masters of Science degree in National Resources Policy from the Industrial College of the Armed Forces, National Defense University, and is a PMI-certified Project Management Professional (PMP).

Elysa Jones
Engineering Program Manager, Warning Systems, Inc.

Elysa Jones holds a Master of Science Degree in Computer Science from the University of Alabama in Huntsville. She comes to the emergency management community after over 20 years providing contractor support to the Army DoD missile defense program. In that capacity,

her work ranged from data reduction and analysis of phased array sensor data to managing software support for a large-scale computer simulation facility. She was involved in the early IEEE work that led to the TCP/IP standards. For the past eight years, Mrs. Jones has been the Engineering Program Manager for Warning Systems, Inc. in the design, development, and deployment of over 70,000 Tone Alert radios and numerous software-controlled dissemination systems. In this capacity, she has served as a board member for the Partnership for Public Warning, works closely with the Emergency Interoperability Consortium, and chairs the OASIS Emergency Management Technical Committee. This committee developed the first emergency data standard for communicating warnings, the Common Alerting Protocol (CAP) as well as the Emergency Data Exchange Language Distribution Element (EDXL-DE) for defining routing assertions for any emergency data. In February 2006, she was awarded the first annual Leadership in Emergency Interoperability Award granted by the Emergency Interoperability Consortium.

Donna Roy
Director, Enterprise Data Management Office, Office of the CIO, DHS

Donna Roy joined the DHS Office of the Chief Information Officer in December of 2006 as the Director of the Enterprise Data Management Office. Prior to joining DHS, she consulted with the National Biological Information Infrastructure (NBII) Program of the US Geological Survey. Ms. Roy was the Geospatial Program Manager and IT Project Manager for NBII, a distributed, Internet-based architecture for sharing the biological resources for management of biodiversity within the US and abroad. In this role her responsibilities included overall management of the IT infrastructure development based on multiple data and interoperability standards, national and global in scope. The NBII realized significant increase in capability with its SOA framework implementation. In addition, Ms. Roy's team worked with DoD, EPA, FDA USDA, DHS, NIH, DOS, and several non-governmental and international organizations in developing the Geospatial Enterprise Architecture, a geospatial SOA framework for interoperability and standards-based toolkits for rapid application development. Prior to her work at the NBII, Ms. Roy served as the VP of Product Development for a data-centric Fortune 500 firm as well as serving as the VP for the data management division. She has over 20 years of IT experience, culminating her data-oriented, enterprise-wide view for the implementation of standards to increase operational efficiency. She presented numerous papers for NBII and other clients on these and other topics.

Paul Wormeli
Executive Director, IJIS Institute

Paul Wormeli is Executive Director of the IJIS Institute, a nonprofit corporation formed to help local and state governments develop ways to share information among the disciplines engaged in law enforcement and the administration of justice. He has been active in the development of software products, has managed system implementation for dozens of agencies throughout the world, and has managed national programs in support of law enforcement and criminal justice agencies. Mr. Wormeli was the first national project director of Project SEARCH, the National Consortium for Justice Information and Statistics, and was subsequently appointed as Deputy Administrator of the Law Enforcement Assistance Administration in the U.S. Department of Justice. His experience covers all phases of the criminal justice system. Mr. Wormeli holds a Bachelor's degree in Electronics Engineering from the University of New Mexico and a Master's degree in Engineering Administration from George Washington University.

Breakout Series II: Session A: P25/CAP: What Does It All Mean?

Eric Nelson
Electronics Engineer & Team Leader, Interoperability Research Laboratory Institute for Telecommunication Sciences (ITS)

Eric Nelson has 12 years of telecommunications engineering experience. Presently he serves as an Electronics Engineer and team leader of the Interoperability Research Laboratory at the Institute for Telecommunication Sciences (ITS) in Boulder, CO. Last year ITS was charged by the National Institute of Standards and Technology's Office of Law Enforcement Standards (NIST/OLES) to construct the technical components of a Project 25 Compliance Assessment Program. Mr. Nelson holds an MSEE degree from the University of Washington in Seattle where he specialized in applied electromagnetics.

Dereck Orr
Program Manager, Public Safety Communications System, National Institute of Standards and Technology (NIST)

Dereck Orr is the Program Manager for Public Safety Communication Standards at the National Institute of Standards and Technology's (NIST) Office of Law Enforcement Standards, and has held that position since December 2002. From October 2003 until October 2004, Mr. Orr was detailed to DHS to serve as the Chief of Staff of the SAFECOM Office within the Science and Technology Directorate, to help establish the new program. Prior to working at NIST, Mr. Orr served as a professional staff member of the Senate Appropriations Subcommittee for the Departments of Commerce, Justice, and State, and related agencies, under Senator Fritz Hollings. In that position, he was responsible for the appropriations accounts relating to state and local law enforcement issues. Mr. Orr served in that position from July 2001 to December 2002. Prior to that, Mr. Orr served four years at the Office of Community Oriented Policing Services (COPS) at the Department of Justice. At COPS, he held positions as a management analyst, then as Special Assistant to the Principal Deputy Director, and finally as Budget Officer of the COPS Office. Mr. Orr received a Masters in Public Policy from the College of William and Mary and a Bachelor of Arts in American History from the University of Texas at Austin.

Breakout Series II: Session B: VoIP: What It Can Be

DJ Atkinson
Lead Electronics Engineer, National Telecommunications and Information Administration (NTIA), Institute for Telecommunication Sciences (ITS)

DJ Atkinson has been with the Institute for Telecommunication Sciences for almost 20 years, and is currently a Lead Electronics Engineer in the Telecommunication Systems Planning Division. Much of that time, Mr. Atkinson has worked with both IT systems and voice telecommunication systems, so it was a natural for him to get involved with VoIP. Mr. Atkinson is a relative newcomer to the needs of the emergency responder community, having worked for eight years to ensure their needs are met.

Linda Fuchs
Program Manager, Department of Management Services, Enterprise Information Technology Services, State of Florida

Linda Fuchs is a Project Manager with the State of Florida's Enterprise Information Technology Services. In her 20 years with the State, she has spearheaded several enterprise, statewide programs including an interlibrary cooperation network, an interlibrary loan network, and an ERP system. After September 11, 2001 she was asked to manage the Statewide Law Enforcement Radio System (SLERS) project which now provides a statewide 800 MHz system for all state law enforcement agencies and local and Federal third-party subscribers. In 2003, Ms. Fuchs initiated the development of the Florida Interoperability Network (FIN) which uses a ROIP radio network and mutual aid channels throughout the state to provide interoperability for state, local, Federal and Native American first responders. She has an MBA with a concentration in Information Systems Management and a Masters in Library and Information Sciences. She is a certified Project Management Professional. Prior to moving to Florida she worked at the Library of Congress and New Jersey State Library.

Luke Klein-Berndt
Chief Technical Officer, Office for Interoperability and Compatibility, DHS

Luke Klein-Berndt has been the Chief Technology Officer at the DHS OIC for the past six months. Previously, he was at the Office of Law Enforcement Standards (OLES) at the National Institute of Standards and Technology (NIST). While working as a researcher at NIST, he developed a PDA-based test bed to investigate using Voice over Internet Protocol (VoIP) over wireless ad hoc networks. While working to standardize ad hoc networking protocols, he began investigating how they could be used to improve public safety's ability to communicate. Within DHS, Mr. Klein-Berndt leads OIC's efforts to improve communication interoperability through standardization, including the Project 25 suite of standards, broadband communication, and VoIP. In addition, he leads many of OIC's technical efforts, such as the development of both pilots and new tools to assist public safety.

Robert Kuzma
Captain, San Francisco Fire Department

Robert Kuzma is a Captain in the San Francisco Fire Department and for the last eight years has provided Project Management and Risk Assessments for the City and County of San Francisco. His current projects emphasize Communications Interoperability and Development of Infrastructure to provide Enhanced Situational Awareness. Captain Kuzma is a participant in the development of the San Francisco and 11 County Bay Area Regional Tactical Interoperability Communications Plans (TICP). He also is the Designer and Project Manager for the construction of an Incident Command Vehicle (ICV), which is designed to support a Unified Command at the scene of complex incidents. The vehicle will serve as a development platform to showcase emerging technologies, including the integration of commercial satellite and cellular data networks to provide access to VOIP and Application Service Providers (ASP). Captain Kuzma is the Designer and Project Manager for the Fire Department Operations Center (FDOC), which functions as the Department's Intelligence and Information (I&I) section under the National Incident Management System (NIMS). He is a consultant for the designs of the Operations Centers for the Department of Public Health, Police Department, and Department of

Emergency Management, and is Project Co-Manager for the deployment of a Tactical 4.9 GHz MESH data network and wireless cameras to provide enhanced situational awareness at the 2007 Baseball All-Star Game. He is also Project Co-Manager for the design and implementation of the San Francisco Public Safety enhanced Wireless Data Network Project. This project will upgrade the current City Wide Data-TAC Network to a Wireless Broadband Mesh Network. As a Consultant to the Mayor's Office of Criminal Justice for the $23 million 2003 UASI Grant, he analyzed all City and County Technology and Communications Project proposals and provided funding recommendations. Captain Kuzma was the recipient of the 2004 Mayor's Fiscal Advisor Committee (MFAC) Award for the implementation of SFStat, which included the use of GIS to map 911 service requests densities and provide trends analysis. He received his B.A. from Vassar College.

Breakout Series III: Session A: National Interoperability Baseline Study: So What?

Troy Cribb
Majority Counsel, Senate Committee on Homeland Security and Governmental Affairs

Troy H. Cribb is counsel to Senator Joseph I. Lieberman on the Senate Committee on Homeland Security and Governmental Affairs. Ms. Cribb's portfolio includes Federal financial management and procurement policies as well as a variety of issues relating to DHS, including emergency communications. Prior to joining the Committee, Ms. Cribb was Trade Counsel in the international trade practice of Steptoe & Johnson LLP. She previously served in the Clinton Administration as a Deputy Assistant Secretary of Commerce in the International Trade Administration and as Assistant Secretary of Commerce for Import Administration. Ms. Cribb began her career as a legislative aide to Senator Ernest F. Hollings and then as a staff member of the Senate Committee on Commerce, Science, and Transportation. Ms. Cribb has an undergraduate degree from Northwestern University and a law degree from Georgetown University.

Tony Frater
Deputy Director, Office for Interoperability and Compatibility, DHS

Bio included in the Grant Guidance: What You Need to Know section

Véronique Pluviose-Fenton
Majority Senior Counsel, House Committee on Homeland Security

Véronique Pluviose-Fenton is the Policy Director for the House Committee on Homeland Security. Prior to her employment on the Committee, she served as the Principal Legislative Counsel at the National League of Cities where she concentrated on federalism related issues and homeland security. As Legislative Counsel in the U.S. House of Representatives in the 1990s, she worked on issues arising from the Committee on the Judiciary, including the impeachment of President William Jefferson Clinton. Prior to her Capitol Hill experience, she worked in the area of civil rights at the U.S. Commission on Civil Rights and the NAACP Legal Defense and Educational Fund, Inc. She is a graduate of the City College of New York and received her *juris doctor* from the University of Virginia School of Law.

Victoria Velez
Director,Office of Emergency Communications, DHS

Bio included in the Major Speakers section

Marilyn Ward
Executive Director, National Public Safety Telecommunications Council (NPSTC)

Marilyn Ward is the Executive Director for the National Public Safety Telecommunications Council. Ms. Ward brings 33 years of experience as both an advocate for public safety telecommunications issues and as an administrator in public safety telecommunications, from her position as Manager of Communications at the City of Orlando and part-time police officer in her early days in public safety to her role as Orange County Public Safety Communications Manager, from which she retired in 2005. She served as the Orange County, Florida, Communications Manager until March 2005. Appointed September 1999, Ms. Ward served in Orange County, Florida, managing 9-1-1, Radio Services, and Government Information. She was the project manager for the 3-1-1 Project and is the Chair of the Governor's Statewide Regional Domestic Security Task Force Interoperability Committee. As Communications Manager, Ms. Ward was able to stay involved with communications issues on every level—local, state, and Federal. Ms. Ward served as the APCO Task Force Leader on the Public Safety Wireless Advisory Committee (PSWAC) and was instrumental in creating the National Public Safety Telecommunications Council (NPSTC), the follow-on effort to provide a unified voice for public safety telecommunications needs. She is a member of the Radio Club of America and former president of the Association of Public Safety Communications Officials – International (APCO) and NPSTC Chair. Ms. Ward holds a degree in Business and Management and has received many public safety-related certificates in her career.

Breakout Series III: Session B: Public Safety Broadband: Can It Really Work?

David Boyd
Director, Command, Control and Interoperability, DHS

Bio included in the Major Speakers section

Christopher Guttman-McCabe
Vice President, Regulatory Affairs, CTIA

Since joining CTIA in May 2001, Christopher Guttman-McCabe has worked on a wide range of issues involving spectrum, regulatory mandates, and homeland security. As the Vice President for Regulatory Affairs for the Association, he is responsible for coordinating regulatory issues affecting the wireless industry. Prior to joining CTIA, Mr. Guttman-McCabe worked as an attorney for four years at the D.C.-based law firm Wiley Rein LLP. He served as an Associate in the Communications Practice Group where he advised clients on wireless and common carrier issues, including licensing, compliance, and policy matters. He started his career as a management and strategic consultant to the steel industry at AUS Consultants and later co-

founded Jacobson & Associates, a metals industry management and strategic consulting firm, where he served as the Vice President. Mr. Guttman-McCabe received his B.A. degree in Economics from Swarthmore College and his J.D. Magna Cum Laude from Catholic University with a certificate from the Institute for Communications Law Studies.

Gregory Henderson
Manager of Broadband Technology, Tyco Electronics Wireless Systems Segment

Dr. Gregory Henderson is the manager of broadband technology for Tyco Electronics Wireless Systems Segment where he is responsible for the development of M/A-COM's (Tyco Electronics) 4.9 GHz broadband wireless products. In addition, Mr. Henderson is responsible for M/A-COM's standards activities for public safety broadband wireless solutions through both the WiMAX Forum (working towards the adoption of a standard profile for WiMAX services in the 4.9 GHz band) and in TIA, where he is currently the Vice-Chair of the APCO P25/34 Interface Committee on Broadband Data (working on the development of standards for 4.9GHz networks). He is also M/A-COM's chief technical liaison with the FCC on 4.9 GHz broadband regulatory matters. Mr. Henderson received his Ph.D. from Georgia Institute of Technology in Electrical Engineering in 1993. Since this time he has worked at M/A-COM), TriQuint Semiconductor, and IBM on the development of technologies and products (from semiconductor products to system solutions) for wireless communications applications. He has published over 40 journal and conference publications, mainly focused on wireless communications.

Robert LeGrande II
Interim Chief Technology Officer, Office of the Chief Technology Officer (OCTO), District of Columbia

Robert LeGrande II has been selected to serve as the interim director of the Office of the Chief Technology Officer for the District of Columbia. Mr. LeGrande is a seasoned IT professional with a diverse history of executive-level managerial experience in both the corporate and municipal arenas. His unique career trajectory has afforded him the opportunity to demonstrate proficiencies in operational and financial management; program design and implementation; project and account management; and sales and marketing. Mr. LeGrande has served as deputy chief technology officer for the municipal government of the District of Columbia. In this capacity, he provided leadership for the city's Wireless Network Operations, Human Services Modernization Program (HSMP), Citywide Credentialing, and the National Capitol Region's Interoperable Communications Program. Under his direction, the Nation's first citywide broadband wireless network for first responders has been implemented. This pilot network serves as a test bed for how applications can be shared securely among public safety agencies and provides insight to key requirements and operational issues regarding broadband technology. Similarly, the HSMP will upgrade and integrate IT applications across human services agencies throughout the District of Columbia. To forward the effort of the Public Safety Wireless High Speed Data Network Program, Mr. LeGrande spearheaded the creation of the Spectrum Coalition for Public Safety to secure additional 700 MHz spectrum for public safety communications. In addition, Mr. LeGrande oversees the establishment of a comprehensive data solution for public safety and first responders under the National Capital Region's Interoperability Program. This program will allow all agencies in the District of Columbia, Northern Virginia, and Maryland to share information concerning incidents that affect the region and allow for unified response and support from multiple jurisdictions on a real-time basis. Mr.

LeGrande's vision is to establish a technology platform to support voice and data interoperability.

Harlin McEwen
Chairman, Communications and Technology Committee, International Association of Chiefs of Police (IACP)

Harlin R. McEwen has been in the field of law enforcement for over 49 years. He has served as a Patrol Officer, Investigator, Sergeant, Lieutenant, and Chief of Police. After serving as Chief of the Cayuga Heights (NY) Police Department, he served as Deputy Commissioner of the New York State Division of Criminal Justice Services where he was responsible for overseeing training and registration of all police officers and peace officers in New York State. He then served as Chief of Police for the City of Ithaca (NY) where he was instrumental in implementing modern technology and computerization, and advancing training and professionalism of the force. In 1996 he retired from his position as Chief and was appointed as a Deputy Assistant Director of the Federal Bureau of Investigation (FBI) in Washington, DC where he provided executive oversight for new FBI Criminal Justice Information Services such as the National Crime Information Center (NCIC) 2000 Project and the Integrated Automated Fingerprint Identification System (IAFIS). In April 2000, he retired from the FBI and active law enforcement service and was presented the prestigious FBI Medal of Meritorious Achievement by FBI Director Freeh. In November 2000, the International Association of Chiefs of Police (IACP) at their Annual Conference in San Diego honored Chief McEwen by presenting him with the first IACP Lone Star Distinguished Award in recognition of his exemplary service to the IACP as Chairman of the IACP Communications & Technology Committee. He continues to serve as Chairman of the Communications & Technology Committee of the IACP, having served in this capacity for more than 28 years. He also serves as Communications Advisor to the Major Cities Police Chiefs Association, the National Sheriffs' Association, the Major County Sheriffs' Association, and as an advisor to the FBI, the National Institute of Justice, the U.S. Department of Homeland Security and various other local, state, and Federal agencies. He is a member of DHS SAFECOM Executive Committee and currently serves as Vice Chair of the National Public Safety Telecommunications Council (NPSTC) and is a member of the U.S. Department of Justice Global Advisory Committee (GAC) and the Global Executive Steering Committee. He is a graduate of the FBI National Academy and the FBI National Executive Institute. Chief McEwen is a Life Member of the International Association of Chiefs of Police, the National Sheriffs' Association, the New York State Association of Chiefs of Police, and the Association of Public-Safety Communications Officials-International (APCO). Chief McEwen has written numerous articles and lectured extensively throughout the United States and internationally. Chief McEwen was elected Honorary President of the International Association of Chiefs of Police during the Annual Conference held in Boston in October 2006. This was only the second time in the history of the Association that a person has been named Honorary President. He is a Fellow in the Radio Club of America and at the 2006 Annual Dinner Meeting of the RCA was honored by being named the first recipient of the RCA/NPSTC Richard DeMello Award for his many and longstanding contributions to public safety communications.

Morgan O'Brien
Co-founder and Chairman, Cyren Call Communications

Morgan O'Brien is a co-founder and Chairman of Cyren Call Communications, a new venture seeking to create a nationwide, seamless, broadband network for public safety communications. He was the co-founder of Nextel Communications, Inc. in 1987 and served as its Chairman from 1987 to 1995 and vice-chairman until its merger with Sprint Corporation in 2005. A pioneer who has helped shape the wireless industry and changed the way Americans communicate, Mr. O'Brien was honored by RCR Wireless News and inducted into the Wireless Hall of Fame. Along with Nextel co-founder Brian McAuley, Mr. O'Brien helped transform the SMR industry into a major wireless player. Mr. O'Brien began his career as a lawyer with the Mobile Services Division of the FCC in 1970 where he assisted in establishing the rules and procedures for all land mobile services. Later, he practiced communications law and from 1986 to 1990 was the Partner-in-Charge of the telecommunications practice at Jones, Day, Reavis & Pogue. Known for his innovation and willingness to take risks, Mr. O'Brien was recognized in 1987 as New Jersey Entrepreneur of the Year and in 1993 he was voted the RCR Person of the Year. He was also named RCR Person of the Year in 2006. Recently, he was inducted into the Washington Business Hall of Fame. Mr. O'Brien's interests extend to his support of community. He currently serves as Chairman of the Board of Trustees of The Field School in Washington, DC and as a member of the Law Board of Northwestern University School of Law.

John Powell
Chair, Interoperability Committee and Software Defined Radio Working Group, National Public Safety Telecommunications Council (NPSTC)

John Powell has over 25 years of law enforcement experience at both the municipal and state levels as a police officer and supervisor for two San Francisco area agencies. During his career, Mr. Powell implemented and/or managed several major projects including a statewide trunked radio system and an E-911 computer-aided dispatch center for the University of California. He has served on numerous local, state, and national committees, including the California Law Enforcement Mutual Aid Radio System (CLEMARS) Executive Committee; the California Legislature's Joint Committee on Fire, Police, Emergency and Disaster Services; and the FCC's Public Safety Wireless Advisory Committee (PSWAC). He has also served as chair of the Interoperability Subcommittee of the FCC's 700 MHz Public Safety National Coordination Committee (NCC). He has testified before numerous legislative bodies at all levels of government. While concentrating in the area of wireless telecommunications, he has had a wide range of responsibilities in administration, crime prevention, emergency management, explosive ordinance disposal, operations, personnel, project and records management, public information, training, and strategic planning. He has consulting experience with high-security access control for the National Aeronautics and Space Administration (NASA) and wide-area satellite communication systems for the State of California. Since leaving the University of California in 2002, Mr. Powell, a senior consulting engineer, has consulted extensively on issues and projects related to advanced telecommunications technologies, including interoperability and software-defined radio, for the U.S. Department of Homeland Security, the U.S. Department of Justice, and the Executive Office of the President of the United States. He currently chairs California's FCC-chartered Statewide Interoperability Executive Committee (SIEC) and the Interoperability Committee and Software Defined Radio Working Group within NPSTC. He is the government representative to the Board of Directors at the Software Defined Radio Forum, a member of the Executive Committee of Project SAFECOM within the U.S. Department of Homeland Security, and the Project 25 Steering Committee. He is one of four recipients of

APCO's Art McDole Award for long-term technical contributions to the art and practice of public safety telecommunications and was named "Most Influential Person in Public Safety Spectrum Management" by *Radio Resource* magazine in 1998. Mr. Powell has authored numerous articles for communications sector publications on operational and technical issues related to advanced wireless communications, interoperability, and software-defined radio.