Statement for the Record

David G. Boyd, Ph.D.
Director
Command, Control and Interoperability Division
Science and Technology Directorate
U.S. Department of Homeland Security

Before the U.S. House of Representatives
Committee on Appropriations
Subcommittee on Homeland Security

March 17, 2009

Introduction

Good morning Chairman Price, Ranking Member Rogers, and Members of the Subcommittee. Thank you for inviting me to speak with you today about interoperable communications and our efforts to ensure emergency responders have the information they need to effectively respond to natural and man-made disasters.

Since the creation of the U.S. Department of Homeland Security (DHS), there has been considerable progress in strengthening interoperable communications across the Nation. The Science and Technology (S&T) Directorate has been at the forefront of efforts to improve interoperable communications since 2003 when the SAFECOM program was transferred from the Federal Emergency Management Agency (FEMA) to S&T. SAFECOM worked directly with emergency response and preparedness agencies by coordinating directly with local, tribal, state, and Federal agencies. SAFECOM later became a part of S&T's Office for Interoperability and Compatibility (OIC), which was established by Congress in 2004 and is housed within S&T's Command, Control and Interoperability (CCI) Division. OIC also became heavily involved in data communications when the Disaster Management (DM) program became part of OIC in 2005.[1]

OIC is responsible for improving voice and data communications for the emergency response community by piloting new technologies; developing and disseminating best practices, lessons learned, case studies, and other tools; testing and evaluating current technologies; and creating methodologies for establishing a system of systems nationwide. OIC adopted SAFECOM's practitioner-driven approach to strengthen and integrate interoperability and compatibility efforts.

In FY 2007, elements of the SAFECOM program were transferred from S&T to the DHS Office of Emergency Communications (OEC). Both offices work in partnership to ensure the continued success of the SAFECOM program, with OIC responsible for research, development, testing, and evaluation (RDT&E), and standards development efforts. OIC also supports the implementation of statewide communication interoperability plans in all 56 states and territories, and created the Statewide Communications Interoperability Plan scorecard used to help all levels of government measure their current state of interoperability and lay the foundation for establishing accountability for future progress. (For more information on specific tools, see Appendix A).

CCI focuses on ensuring homeland security practitioners[2] have the necessary information to make critical decisions. The need for relevant, real-time, and actionable information is critical during emergency response operations and is the unifying force for all of CCI's efforts. Having access to the right information at the right time is vital to making tactical, strategic, and planning decisions that can prevent terrorist attacks, protect the homeland from natural or man-made disasters, improve response and recovery, and strengthen the resiliency of our communities by

[1] Elements of DM were transferred to the Federal Emergency Management Agency in 2006, but OIC maintains responsibility for accelerating data messaging standards.

[2] Homeland security practitioners refer to the end-user community that supports all aspects of securing the homeland, encompassing local, tribal, state, and Federal emergency response practitioners; industry; academia; and international partners.

ensuring the information needed to restore the homeland and its critical infrastructures is readily available when needed.

The tools we have developed are already in wide use throughout the United States and Canada and some have even been adopted by the United Kingdom.

CCI manages a robust stakeholder network and creates forums to gather direct input from homeland security practitioners. This input ensures CCI's investments can be immediately and directly leveraged by the broad homeland security community.

Current Environment

Before I explain the CCI strategy and outline our successes, I would like to describe the nature of interoperability in the United States and explain some of the issues.

The existing public safety communication systems in the United States represent, conservatively, an investment of more than $100 billion, and this figure does not include staffing, maintenance, or training. Clearly, replacing all of these systems (even if we could afford it) would require a decade or more. But there are viable alternatives that can get us where we want to go as a Nation.

I think we can all imagine a communications environment in which every emergency responder was able to talk to whomever they needed to, when they needed to, and when properly authorized to do so. In this ideal world we would expect each officer and each of our agency leaders and public officials to be able to communicate effectively using whatever communications devices they had at hand—a desktop telephone or computer, a cell phone, a PDA or other handheld communications device, or a vehicle mounted radio. We can imagine they would also be able to communicate not just by voice, but would also be able to exchange data, imagery, maps, and high definition video and would be able to combine all of these sources of information in whatever way we needed to address an emergency.

While no agencies today have all of these capabilities, all of the foundation technologies required to achieve these things already exist. We have the Internet, satellite communications systems, cellular telephone systems, Blackberries, and our desk and notebook computers. CCI has already demonstrated ROW-B (Radio Over Wireless–Broadband) right here in the District—a system which provides all of these communications capabilities, if agencies can afford them.

But while technologies with all these capabilities exist now and offer real advantages to emergency responders, many of them are dependent on commercially based systems which are necessarily designed to meet essential commercial requirements such as affordability. That means the systems are sometimes too fragile for major disasters, as we saw in Hurricane Katrina and on September 11 when both cellular and wired telephone systems were taken out of service. Because these commercial systems cannot afford to provide coverage where there are not enough subscribers to pay the freight, or provide the kind of overcapacity required in an emergency, we depend on public safety systems to operate when all else fails. We need to take advantage of commercial capabilities, but we also must ensure that our systems can degrade gracefully in an

emergency. Once we have lost the Internet and the ability to exchange data with handhelds, cellular telephones, Blackberries and other public telecommunications systems, we will still need to make sure that at least voice communications remain available to emergency responders. That means strengthening state and local public safety communication systems, not just trying to replace them with single solutions that may not work in all cases.

CCI Philosophy

CCI's guiding philosophy is fostering a strong link to the practitioner community. CCI manages a robust stakeholder network and creates forums to gather direct input from homeland security practitioners. This input ensures CCI's investments can be immediately and directly leveraged by the broad homeland security community.

In 2007, CCI met with representatives from major organizations representing emergency responders and associated stakeholders, including the International Association of Chiefs of Police, International Association of Fire Chiefs, National Governors Association, and National Association of Counties. The meeting resulted in a group consensus around principles that are essential to achieving interoperability. CCI has incorporated these principles into its shared vision with the emergency response community. CCI strives for:

- An integrated system of systems, in regular use, which allows emergency response personnel to communicate (via voice, data, and video) with whom they need on demand, in real time, and as authorized.
- The ability for emergency responders to respond anywhere, bring their own equipment, and operate on any network immediately, when authorized.
- The capability for emergency responders to use the networking and spectrum resources needed to function properly.
- A system of systems approach that will allow response agencies the flexibility to select equipment that best fits technical requirements and meets budget constraints while still achieving interoperability.

Given this shared vision, the cornerstones of CCI's strategy to work with the emergency response community include:

- Mission-critical voice is primary; data is secondary, but very important.
- Interoperability begins with—and its greatest value is realized in—daily use by local users.
- Interoperability is both a technical connection and an effective shared understanding. It is imperative that we not forget the crucial human element. No matter how good a technology is, no matter how impressive the systems produced are, unless the first responders themselves in each of these agencies support interoperability across agency and disciplinary boundaries and are willing to build everything from standard operating procedures to governance charters, we cannot make it work.
- The Federal Government must coordinate its interoperability efforts, and partner with users at all levels, to ensure Federal agencies can interoperate with local, regional, state, and tribal agencies. Solutions must offer added value to the agencies the Federal Government is trying to serve.

- Any solution developed or implemented for public safety purposes must be affordable not just to purchase but also to maintain.
- All levels of responders, policymakers, industry, and the public will be educated on the ways interoperable communications can save lives, money, and property.
- Grant funding authorizations and conditions from states and the Federal Government are prioritized to support cooperative efforts over the strengthening of stand-alone systems.
- Agencies struggling with the issue of operability should strongly consider the long-term benefits of joining regional interoperability initiatives and partnering with neighboring agencies in the planning and acquisition of a communications system.
- A strategy must permit interoperation among existing systems and help agencies build rational migration strategies to new systems that will both improve their capabilities and fit in the larger national objectives.
- CCI must provide not just the new widget that we developed in the Nation's laboratories, but also provide all that is required to put a system or technology in place—training and training programs, technical assistance, expert guidance, and commercialization assistance to the industries we need to build these capabilities.

Strategic Approach

To put CCI's philosophy into action, the Division structures its efforts around building a toolkit that will help practitioners gather, manage, analyze, share, and protect information. CCI is continuing to develop and strengthen this toolkit to transform new and promising concepts—including technologies, processes, methodologies, and standards—into real, viable capabilities. The toolkit will enable automated knowledge management capabilities that can identify and analyze potential national threats, strengthen data and voice communications interoperability, provide easy-to-use data fusion technologies, improve public alerts and warnings, enhance the security and integrity of the Nation's cyber infrastructure and the Internet, and lead to the development of an integrated network of sensors and investigative tools.

The CCI toolkit is a scalable and repeatable model enabling data collection, and the integration of disparate information applications that can be displayed through a single visual platform. The toolkit will improve comprehensive, timely threat awareness and informed decision making. Ultimately, this work will allow agencies across the Nation to make critical information actionable in partnership with other local, tribal, state, and Federal agencies before, during, and after an incident.

The response community is very conservative when it comes to adopting technologies or new operational concepts, because their first objective is to protect the lives and property of the public. CCI's focus on pilots allows it to effectively introduce the new technologies and further refine technologies and concepts before they are rolled out nationally.

Experience shows that the first requirement in introducing any new technologies or approaches is to first establish credibility by proving they really work in an operational environment. CCI's "working circle" concept takes advantage of the fact that every community has a circle of neighboring jurisdictions with whom they are used to working. When CCI introduces a new

technology or technology-based approach, a pilot demonstration is conducted, ideally of several months duration, with a willing agency.

A single pilot demonstration in a single locality rarely generates sufficient information to develop a replicable model for the Nation. Because every jurisdiction, community, and geographic area in the United States is different, and has different needs and problems, CCI conducts these pilot and demonstrations in as many places as possible. Therefore, the pilot demonstrations affect not just the communities in which they are conducted, but also influence their neighbors and working circles, ultimately speeding adoption of technologies and lessons learned across the Nation.

Once CCI is able to prove that the piloted concepts and technologies work in an actual operational environment, CCI's partners in the pilots become the most valuable advocates for the new technologies. It is not an exaggeration to suggest that declaring "we're from Washington and we're here to help" is often less than reassuring to local agencies who often doubt that federal experience and qualifications are relevant to their day-to-day operations.

CCI Technologies

CCI has worked on many levels to move the country toward interoperability. Collectively, CCI has collaborated with other Federal entities to successfully:

- Define interoperability and the challenges of interoperability through the National Task Force on Interoperability.
- Create consistent ways to improve interoperability beyond technology only, through tools like the Interoperability Continuum.
- Measure the state of interoperability to show progress and the work that remains.
- Gain focused funding for interoperability through Federal grant programs and coordinated grant guidance.
- Demonstrate, pilot and transition a multitude of tools, technologies, standards, and methodologies for use in the emergency response community.
- Influence communities and associations to begin incorporating interoperability into daily response efforts and in emergency response planning efforts.
- Facilitate the development of innovative communications systems that meet end-user needs and advance interoperable communications technologies.

While governance and other human dimensions of interoperability are critical to any solution, technology remains at the center of the issue, making research, development, testing, evaluation and piloting of new interoperable technologies vital to the creation of a comprehensive solution. CCI is leading the way on the development of numerous technologies, many of which are currently being successfully piloted throughout the Nation. Examples include:

Critical Infrastructure Inspection Management System (CIIMS)
When the Maryland State police were faced with the challenge of conducting regular and systematic inspections of critical infrastructure in the state, they reached out for help. Their challenge was that conducting these inspections was resource-intensive and could only be accomplished from the air. Existing critical infrastructure information was

collected in paper files – a major roadblock to data interoperability. To answer Maryland's request, CCI formed a team with the Applied Physics Laboratory at Johns Hopkins University to develop a tablet computer system that allows air crews to efficiently manage inspections of important critical infrastructures and exchange relevant information with their partners on the ground—CIIMS.

The most serious challenge was cost. Introducing any new technology in an aircraft is extraordinarily expensive, commonly costing more than $100,000 per airframe. By using appropriate off-the-shelf technology, such as the GPS capability on the aircraft itself that is supported by the Federal Aviation Administration's flight following system, and by developing some specialized software, we were able to field a system which meets Maryland's critical inspection requirements and permits the sharing of critical data with both state and Federal agencies. On top of all this, we did it with a solution that costs a fraction of any other aircraft installed alternative and which Maryland estimates already saves them more than a quarter of a million dollars a year.

Recently, the Los Angeles Police Department (LAPD) was made aware of CIIMS and requested CCI's assistance in implementing the technology in aircraft as well as developing a terrestrial version that could be used in patrol cars and other emergency vehicles. The result is a program the LAPD calls LA Shield. LA Shield will enable more rapid and expanded adoption of CIIMS technology across the Nation.

Multi-Band Radio

Traditionally, emergency response radios were built to operate within a single radio band. Therefore, most local, tribal, state, and Federal emergency response agencies must rely on the use of several single-band portable or mobile radios to maintain a level of interoperability with partner agencies. While some agencies swap or share radios, others employ time-consuming methods to exchange information, including relaying messages through dispatchers or using runners to hand-carry messages. To address these challenges, OIC worked with the emergency response community and its partners at FEMA and OEC to identify requirements for a multi-band radio (MBR). OIC is partnering with industry to test and demonstrate a prototype multi-band, multi-mode portable radio capable of providing uninterrupted communications between emergency response agencies operating in the public safety radio bands.

The MBR is equal in form, factor, and cost to existing high-end portable radios. However, the MBR equips emergency responders with the unprecedented capability of operating across the entire range of public safety radio bands. To communicate with another agency, users simply select the assigned channel.

In early January 2009, OIC received the initial delivery of 10 prototype MBRs for lab testing and short- and long-term demonstrations. Preliminary lab testing is being conducted by the National Institute of Standards and Technology (NIST) and includes law enforcement, fire services, rescue, emergency medical services (EMS), and emergency management agencies at the local, regional, state, and Federal levels. NIST is leading the validation of equipment specifications and will conduct compliance testing relative to existing voluntary consensus standards. Additional lab testing is occurring

with the National Interagency Fire Center and the Boise, ID Fire Department, in cooperation with the U.S. Department of Agriculture's Forest Service. OIC is also working with the following agencies in the New York City metropolitan area to test and evaluate the MBR: the Fire Department of New York, New York City Department of Information Technology and Telecommunications, New York Police Department, Office of Emergency Management, and Port Authority of New York and New Jersey.

OIC will also conduct short-term demonstrations and pilots of the MBR. Michigan EMS, a state organization, will conduct short-term demonstrations and testing across Michigan. In the fall, long-term pilots will be conducted at numerous locations across the United States. The MBR project will transition to the user community once detailed testing and evaluation is completed and a final report of the findings is published.

The MBR has the potential to save lives and protect property across the Nation. OIC's efforts have sparked industry's decision to invest in similar technologies to provide emergency responders with additional options when procuring communications equipment.

Virtual Alabama

The State of Alabama approached CCI with a program they developed called Virtual Alabama. Virtual Alabama is a visualization tool which overlays statewide satellite imagery and aerial photography with critical data such as real-time weather information and the location of fire hydrants, pipelines and other information critical to the state in emergency situations. The project continues to be enhanced so that it now is able, while meeting the access concerns of localities (localities need to be able to restrict access to certain data), to display both before and after information on disasters such as last year's tornadoes and floods, architectural data on buildings needed by firefighters, and tax and boundary information of importance to the state in preparing disaster cost information for FEMA as well as in helping to attract business. The only limit to what can be displayed is the imagination of those who draw on the system.

Obviously, a capability like Virtual Alabama has enormous potential. In the coming year, CCI will work with several other states—Alabama, Mississippi, Florida, Texas, Virginia, Kentucky, Tennessee, as well as observers from Georgia, to create both an enhanced and broader, nationwide version of the Virtual Alabama concept. The effort will develop a set of tools that will allow all of the state systems to interoperate and exchange data with each other, regardless of the particular platform or application in use. CCI's goal is to create technologies and methodologies which are both application and platform agnostic and which enable the exchange of information without wasting legacy investments.

OIC is improving interoperable communications through multiple RDT&E and standards development efforts related to land mobile radio (LMR) communications, public safety grade communications networks, and interoperable applications. OIC has prioritized these projects with OEC and FEMA to ensure they provide a significant benefit to the emergency response community. Details regarding additional initiatives OIC and CCI are undertaking to improve communications and interoperability across the Nation are found in Appendix B.

Conclusion

CCI's practitioner-driven approach realized through the information toolkit enables seamless and secure interactions among homeland security stakeholders. This will ultimately result in a communications environment in which every homeland security practitioner is able to talk to whomever, whenever, and as properly authorized to do so. CCI must work to ensure that this environment degrades gracefully to ensure basic operability when all else fails. There are many challenges that lay before us.

CCI's approach has empowered DHS to create tools, resources, and technologies that help the Nation's emergency responders make the most vital decisions and successfully carry out their missions. The tools OIC has developed are in wide use throughout the United States, and last year Canada adopted many of them, including the Interoperability Continuum, a document developed by OIC laying out the five critical success factors for interoperability. At a Canadian Association of Chiefs of Police meeting last month, a representative from the United Kingdom advised me that they have also "borrowed with pride" the Interoperability Continuum and other materials.

Moving forward, CCI will build on its successes to further nationwide interoperability via a system of systems model that leverages skills and abilities of the Nation's homeland security practitioners. Ultimately, practitioners will have the information they need to effectively respond to natural and man-made disasters.

APPENDIX A

The following is a list of tools, best practices, and methodologies[3] developed by OIC that DHS is currently disseminating to local, tribal, state, and Federal emergency responders across the Nation:

- **FY 2003:** Published the first ***Recommended Federal Interoperable Communications Grant Guidance***, which provides guidance for Federal grant programs that fund interoperable emergency communications. Every year since 2003, SAFECOM and OIC have developed recommended grant criteria to help coordinate how funding is allocated, and to maximize the prospects for interoperable communications.

- **FY 2004:** Published the first national emergency response ***Statement of Requirements*** (SoR). The SoR helps align technologies with the needs of emergency responders in the field by defining the requirements—qualitative and quantitative—for crucial voice and data communications in day-to-day, task force, and mutual aid operations.

- **FY 2004:** Designed the **Interoperability Continuum** to help the emergency response community and local, tribal, state, and Federal policy makers address critical elements for success as they plan and implement interoperability solutions. The Interoperability Continuum is now endorsed by the governments of Canada and the United Kingdom.

- **FY 2005:** Published the ***Statewide Communications Interoperability Planning (SCIP) Methodology*** to establish and lead state planning efforts. The SCIP Methodology was critical as all states and territories created their own interoperable communications plans.

- **FY 2006:** Released the ***Operational Guide for the Interoperability Continuum: Lessons Learned from RapidCom*** to share best practices from RapidCom which ensured a minimum level of emergency response interoperability in the top ten high-risk urban areas.

- **FY 2006:** Administered the **National Interoperability Baseline Survey** across the Nation. The study leveraged the Interoperability Continuum to determine and measure interoperable communications nationwide for the purpose of helping the emergency response community make informed decisions about strategies for improving interoperable communications. Results were released in FY 2007.

- **FY 2006:** Published Volumes I and II of the ***Public Safety Architecture Framework*** (PSAF) to help emergency response agencies map system requirements and identify system gaps.

- **FY 2006:** Developed the ***Guide to Standards and Technology*** to demonstrate how DHS works with the emergency response community to define communications requirements and to accelerate standards to help meet those requirements.

[3] These documents are available to local, tribal, state, and Federal emergency responders, policy makers, and the public at www.safecomprogram.gov.

- **FY 2007:** Published the ***Writing Guide for a Memorandum of Understanding (MOU)***, which helps communities interested in establishing formal agreements, such as MOUs, to address multi-organization coordination and communications. The guide includes recommendations for structuring the MOU, questions to consider when compiling content for each section, and sample language to illustrate how a community could write each MOU section.

- **FY 2007:** Released the ***Creating a Charter for a Multi-Agency Communications Interoperability Committee: Template and Questions to Consider*** guide to detail how to create a charter for an interoperability committee or governance group. A charter document describes the reason the group exists and establishes the ground rules of operation. It provides clarity and aligns a diverse group with a common purpose.

- **FY 2007:** Published the ***Writing Guide for Standard Operating Procedures*** to assist communities that are seeking to establish standard operating procedures (SOPs). SOPs are formal written guidelines or instructions for incident response. SOPs typically use both operational and technical components and enable emergency responders to act in a coordinated fashion across disciplines in the event of an emergency. Clear and effective SOPs are essential in the development and deployment of any solution.

- **FY 2007:** Launched the **Computer-Aided Dispatch Interoperability Project** (CADIP) and Case Study pilot. The CADIP team coordinated with emergency response agencies in Silicon Valley, California; Portland, Oregon; and Phoenix-Mesa, Arizona to identify the benefits of seamlessly and securely sharing information between disparate computer-aided dispatch (CAD) systems. The pilot resulted in a published Case Study report and Business Case video.

- **FY 2007:** Developed the **Type III Communications Unit Leader Training** course to train emergency responders how to be radio communications unit leaders during all-hazards emergency operations—significantly improving communications across the multiple disciplines and jurisdictions responding to an incident.

- **FY 2008:** Released the ***Interoperability Business Case: An Introduction to Ongoing Local Funding*** guide, which helps practitioners develop budget justifications that establish the need for dedicated staff and funding for interoperability efforts.

- **FY 2008:** Published the ***Interoperable Communications for Planned Events*** guide to assist practitioners with the coordination of communications assets to enhance communications interoperability during a planned event.

- **FY 2008:** Published the ***Data Messaging Standards Guide for Requests for Proposals (RFPs)*** to assist emergency responders and procurement officers in developing appropriate RFP language requiring data messaging standards when purchasing emergency response-related systems.

- **FY 2008:** Updated the **Interoperability Continuum** to include data communications.

- **FY 2008:** Published the ***Improving Interoperability through Shared Channels*** **Version 2**, which extends and refines the initial document, *Improving Interoperability through Shared Channels* (originally released in February 2007). This updated tool documents three case studies of effective shared channel implementations across the Nation and records lessons learned, obstacles encountered, and best practices. The document provides emergency response officials with a set of key actions that will help guide their shared channel strategy.

- **FY 2008:** Released ***PSAF Volume III***, which describes key data elements that can be used to help emergency response agencies characterize a public safety LMR system, dispatch system, and public safety organization.

- **FY 2008:** Published the ***Plain Language Guide: Making the Transition from 10 Codes to Plain Language*** to help states and localities transition from coded language systems (e.g., 10 codes) to plain language during radio transmissions.

- **FY 2008:** Released the ***System of Systems Approach for Interoperable Communications*** guide to help the emergency response community as well as local, tribal, state, and Federal policy makers understand the system of systems concept, the benefits of applying this concept, and how it can aid agencies in achieving interoperable communications.

- **FY 2008:** Published the ***Computer-Aided Dispatch Interoperability Project Documentation of Regional Efforts***, which presents an overview of how three different regions across the Nation implemented a CAD interoperability project in their region. This document provides emergency responders with best practice recommendations and ideas for how they may be able to link CAD systems in their own region.

- **FY 2008:** Released the **CAD Business Case Video**, which provides high-level decision makers with a value proposition that details the importance of CAD interoperability. The video depicts the same emergency response scenario in two different screens: one with CAD interoperability and the other without. Viewers are able to see how and where in the process significant time is saved. This video also explains *why* this saved time is so critical.

APPENDIX B

OIC and CCI Initiatives

Standards Acceleration

The acceleration of standards is a key component of OIC's approach to strengthening voice and data interoperability. OIC is partnering with emergency responders, Federal agencies, and standards development organizations to accelerate the development of voice and data messaging standards. With these standards, emergency responders are steps closer to having the ability to seamlessly exchange critical information across disparate software systems and applications. In particular, Project 25 (P25) standards are focused on developing radios and other components that can interoperate regardless of manufacturer.

Additionally, OIC is facilitating the development of Emergency Data Exchange Language (EDXL) data messaging standards to exchange critical data, including alerts, hospital capacity, and availability of response personnel and equipment. To date, OIC has published the Common Alerting Protocol (CAP),[4] Distribution Element,[5] Hospital Availability Exchange,[6] and Resource Messaging[7] EDXL standards. These information sharing standards will improve emergency preparedness, response, and recovery efforts.

Project 25 Compliance Assessment Program

To better address the needs of emergency responders, Congress passed legislation calling for the creation of the P25 Compliance Assessment Program (P25 CAP). P25 CAP is a partnership of OIC, the National Institute of Standards and Technology (NIST), and the emergency response community. P25 CAP provides manufacturers with a method for testing their equipment for compliance with P25 standards and to ensure it is capable of interoperating across manufacturers. The first group of laboratory assessments started in December 2008, and should be completed by Spring 2009. P25 CAP will encourage the inclusion of P25 standards in communications systems while creating a means for the emergency response community to confidently purchase and use P25-compliant products.

Voice over Internet Protocol

OIC is also working to improve the bridging devices that emergency responders rely to connect radio systems creating networks. Computer networks are increasingly being used to transmit voice communications among radio systems. This is done using a technology known as Voice over Internet Protocol (VoIP). OIC and NIST established the VoIP Working Group to develop new ways to bridge radio systems. The Working Group developed the Bridging Systems

---

[4] CAP enables the exchange of all-hazard emergency alerts, notifications, and public warnings which can be disseminated simultaneously over many different warning systems (e.g., computer systems, wireless, alarms, television, and radio).

[5] Distribution Element provides a flexible message-distribution framework for data sharing by emergency information systems. Messages may be distributed by specific recipients, by a geographic area, or by other codes such as agency type (e.g., police, fire, and Emergency Medical Services).

[6] Hospital Availability Exchange allows the exchange of information about a hospital, its status and resources, to allow emergency responders and management to make efficient decisions to treat patients.

[7] Resource Messaging provides standard exchange of resource requests for the use, deployment, and return of assets needed to support emergency and incident preparedness, response, and recovery.

Interface (BSI) profile, which enables VoIP communication between bridging/gateway devices that are used to tie existing systems together. To verify interoperability amongst the Working Group participants, OIC has held testing sessions to verify that when using the BSI profile, equipment can communicate with other equipment regardless of the manufacturer. OIC continues to host periodic roundtable discussions to ensure that the BSI and future profiles maintain technical merit and value to the emergency response community. Currently, 13 bridge/gateway manufacturers have voluntarily implemented the BSI profile, with other manufacturers committed to doing so in their next product revision cycle.

Radio Over Wireless-Broadband

In partnership with industry, local government, NIST, and the Institute for Telecommunication Sciences (ITS), OIC has achieved an important communications milestone by demonstrating how to integrate an existing radio system with emerging broadband technologies. Today, many agencies are using LMR systems *and* completely separate wireless broadband systems. Since the LMR and broadband systems serve specific and different needs, they were not designed to communicate with each other. The lack of interoperability between these two separate networks may compromise emergency response operations, as emergency responders communicating on a broadband system are unable to communicate with those responders communicating on an LMR system.

To address this capability gap, OIC launched the Radio Over Wireless Broadband project to research how to connect existing LMR systems with advanced broadband technologies. Broadband technologies, such as Push-To-Talk over Cellular and the Geographic Information System, allow emergency responders to form talk groups and use location-based services for situational awareness and coordination—ultimately saving critical response time. Drawing on the VoIP Working Group's efforts, OIC was able to use the BSI profile to tie broadband technologies with LMR systems.

As industry develops new technologies, it is critical that emergency response agencies are able to integrate them into current and future systems and operations. In addition to supporting the use of bridging interfaces, CCI is also investigating ways to more effectively stream video using similar broadband technologies. Using lessons learned and best practices for effectively integrating LMR and broadband communications systems, OIC will develop replicable tools, resources, and templates that can be used by localities nationwide that are working on similar efforts.

Digital Vocoder Testing

OIC has partnered with practitioners from multiple emergency response disciplines, NIST, ITS, manufacturers, and fire service leaders to understand how background noise affects audio communications. The International Association of Fire Chiefs' (IAFC) Digital Problem Working Group (DPWG) was created to address reports from the field indicating that during light to moderate background noise, the vocoder may slightly distort voice communications. The vocoder is a hardware/software component in every digital radio. The technology uses a speech analyzer to convert voice into a digital signal, and from a digital signal back to audio. In loud background noise scenarios, which can include sirens, helicopters, breathing apparatus, and

alarms, the vocoder may make voice communications completely unintelligible—potentially compromising mission-critical operations.

In June 2008, the *Intelligibility of Selected Radio Systems in the Presence of Fireground Noise: Test Plan and Results* report was published. It provides detailed information related to the first phase of vocoder testing developed and conducted by OIC's partners—ITS and IAFC/DPWG's Testing Subcommittee. The results indicate that in some environments analog radios performed better than digital radios, and in some environments no radios performed well. Fire agencies should consider the first phase of vocoder testing results when preparing to purchase and deploy any new communications system. For the second phase, OIC will determine what technology improvements are needed to overcome background noise issues. Additionally, OIC's partners are also working to identify immediate behavioral, procedural, and technical steps that agencies can take to avoid or minimize emergency response background noise.

Video Quality in Public Safety

From February 3-6, 2009, OIC, NIST, and ITS held the first-ever Video Quality in Public Safety Working Group meeting. The meeting brought together users of public safety video applications to identify the major policy, technology, and practical use challenges of public safety video systems. The conference also served to lay the groundwork for the development of collaborative solutions, a shared language, and the establishment of meaningful and comprehensive standards. The meeting provided a forum to share ideas, solicit input, and gather user needs and requirements. Comprised of public safety practitioners, academics, Federal partners, and vendors, the Working Group is creating an end-user guide to help equip practitioners with the proper framework for thinking about the way they use video. This guide will also help practitioners articulate their needs to vendors when they look to purchase or upgrade video systems.

Commercial Mobile Alert Service

As the Nation becomes increasingly mobile, analog broadcast public alert and warning systems cannot sufficiently reach enough of the population in an effective timeframe. Because more than 80 percent of the American population subscribes to commercial mobile services, mobile devices—including cell phones and pagers—are becoming ideal devices to initially alert the public of imminent threats to life and property. These devices may also be used to alert the public of child abductions and other Presidential warnings. To improve alerting on mobile devices, the Warning, Alert, and Response Network (WARN) Act created the Commercial Mobile Alert Service (CMAS). In response, OIC established an RDT&E program to enable a national capability to deliver relevant, timely, effective, targeted alert messages to the public. At a minimum, the program will improve geographic targeting of alerts and provide more information regarding how the public best responds to alerts and warnings. Once operable, CMAS will effectively alert more people when an emergency occurs.

Integrated Public Alert and Warning System

OIC's success in accelerating the development of EDXL standards makes it a natural partner with FEMA in the Integrated Public Alert and Warning System (IPAWS). OIC is working with FEMA on standards development and adoption, conformity assessment, industry capability analysis, and technology evaluation. IPAWS will eventually enable local, tribal, and state

practitioners to provide reliable and accurate alerts and warnings to more of the public, thus reducing the loss of life and property from all hazards. Recently, OIC actively supported FEMA's adoption of the CAP version 1.1 data messaging standard. CAP provides the ability to exchange all-hazard emergency alerts, notifications, and public warnings, which can be disseminated simultaneously over many different warning systems, including CMAS, the Emergency Alert System, and the National Weather Service All Hazards network.

Virtual City

As part of its strategy to enable a seamless information infrastructure for the emergency response community, CCI is supporting a pilot to demonstrate interoperable voice and data communications, information gathering, and visualization techniques in the City of Beverly Hills, California. This demonstration, known as Virtual City, will integrate data from multiple sources, including cameras, location-sensors, and license-plate readers, and make that information more accessible by displaying it in context with an easy-to-use map viewer. Once complete, CCI will publish a resource guide for state and local law enforcement agencies that will explain the step-by-step process involved in implementing Virtual City. This guide will enable situational awareness technologies and best-practices to be repeated nationwide.

Regional Operational Platform Pilot

With support from CCI, eight southern states are collaborating for the Regional Operational Platform pilot, which is creating a national model for interstate information sharing using visualization platforms. Each state has or is working to develop a visualization tool that meets the emergency preparedness needs for their state. Over the course of the pilot, the states will work to populate their tools with appropriate data and link with other state systems to share information relevant to increasing citizen safety, protecting the critical infrastructure, and maximizing emergency preparedness and response. Once complete, each state's visualization tool will be linked and each state will collaborate through relevant policies and procedures that enable successful cross-state information sharing in support of a safer Nation.