



# Interoperability TECHNOLOGY Today

A Resource For the Emergency Response Community

Winter 2009

## Texas to Improve Emergency Radio Communications Systems with Federal Funding

**D**on't mess with the priorities of Texas—the State is currently using Homeland Security grants to significantly improve emergency radio communications systems. This improved system is projected to use wireless radios that allow local, tribal, state, and Federal agencies to more effectively communicate during natural disasters, critical emergencies, and day-to-day incidents.

Every public safety agency in Texas is expected to be fully compliant with Project 25 (P25) standards by late 2015. P25 standards ensure that radios can interoperate regardless of manufacturer. If this deadline is met, Texas will be one of the first states to accomplish this degree of compliance. The surface area of Texas covers 261,797 square miles, and has 254 counties with more than 5,300 public safety agencies. The task for every agency to be compliant by 2015 with P25 standards will be nothing short of a Herculean undertaking.

What led Texas to align its focus on interoperability and wireless communications compliance? In 2006, the Texas Radio Coalition (TxRC), a group of radio communications system operators and public safety responders from across the State gathered to devise a formal statewide “system of regional systems” plan. In March 2007 the U.S Department of Homeland Security (DHS) released the Statewide Interoperability Planning Guidebook and required each state to submit a Statewide Communications Interoperability Plan (SCIP). The Homeland Security Director in Texas approved the TxRC proposed plan in December 2007 and it received approval from DHS in April 2008. From there, the Governor of Texas, Rick Perry, announced a refreshed vision that aimed to strengthen interoperable wireless communications for every agency in Texas.

Texas made significant strides in developing its SCIP by partnering with the Texas Association of Regional Councils—a group comprised of 24 diverse regional councils of government. The Sheriffs’ Association of Texas also played an instrumental role in the State’s ability to assemble the SCIP in less than six months. In addition to partnering with these coalitions and multiple public safety groups, Texas also drew participation from non-profit groups, tribal governments, and Federal agencies.

“Achieving shared understanding and support for P25 standards compliance among these diverse parties required relentless focus and

persistence,” says Joe Peters, Director of the Technology Assistance Division of the Sheriffs’ Association of Texas. “Part of the challenge for Texas is our vast layout—85 percent of the entire State is comprised of rural territory, particularly regions around the border.”

To address the challenge of promoting interoperability throughout Texas’s large rural expanses, the State acquired Public Safety Interoperable Communications grants. These grants were awarded throughout Texas to regions where projects were identified to enable significant improvement in communications infrastructure. Moving forward, the availability of Federal funds will be contingent on statewide compliance with the approved SCIP.

### Current Challenges, Future Goals

Peters and Mike Simpson, TxRC Coordinator and City of Austin Wireless Communication Services Manager, are leading a group comprised of representatives across 40 counties in an effort to build a new communications system that will span the 1,254 mile length of the Texas border with Mexico. To achieve P25 compliance with this system, two layers of communications must be used: a VHF layer for rural areas, and a 700/800 MHz layer for urban regions. These groups are planning to replace antiquated devices with technologies that will afford emergency response agencies better operability and interoperability—including data sharing capabilities—across those systems. Building this complex interoperable communications system will require cooperation from each of the 40 counties. Sharing this multi-regional system will allow emergency responders to talk with one another from El Paso to Brownsville, an international boarder of 1,254 miles.

Once agencies are able to improve operable voice capabilities and the degree of interoperability and coverage needed by each region is achieved, the next priority will be to tackle the data interoperability technology needs of the new public safety wireless system.

Funding remains a major issue for both rural and urban agencies as they strive to improve statewide interoperability. While Texas has efficiently applied Federal funding to construct and implement a common infrastructure for these groups, Peters and Simpson acknowledge that one large grant will not be enough to sustain the system that the State is currently constructing. Peters says, “This central question remains: In the future, how will we maintain the infrastructure we are implementing now? Will there always be maintenance funding for an infrastructure of this magnitude?”

The multitude of Texas’s rural counties—whose budgets tend to be smaller—also contributes to the challenge of funding. To maintain the complex infrastructure, emergency response groups are working with State legislators to establish a recurring State funding plan.

### Texas Coastal Communications Project

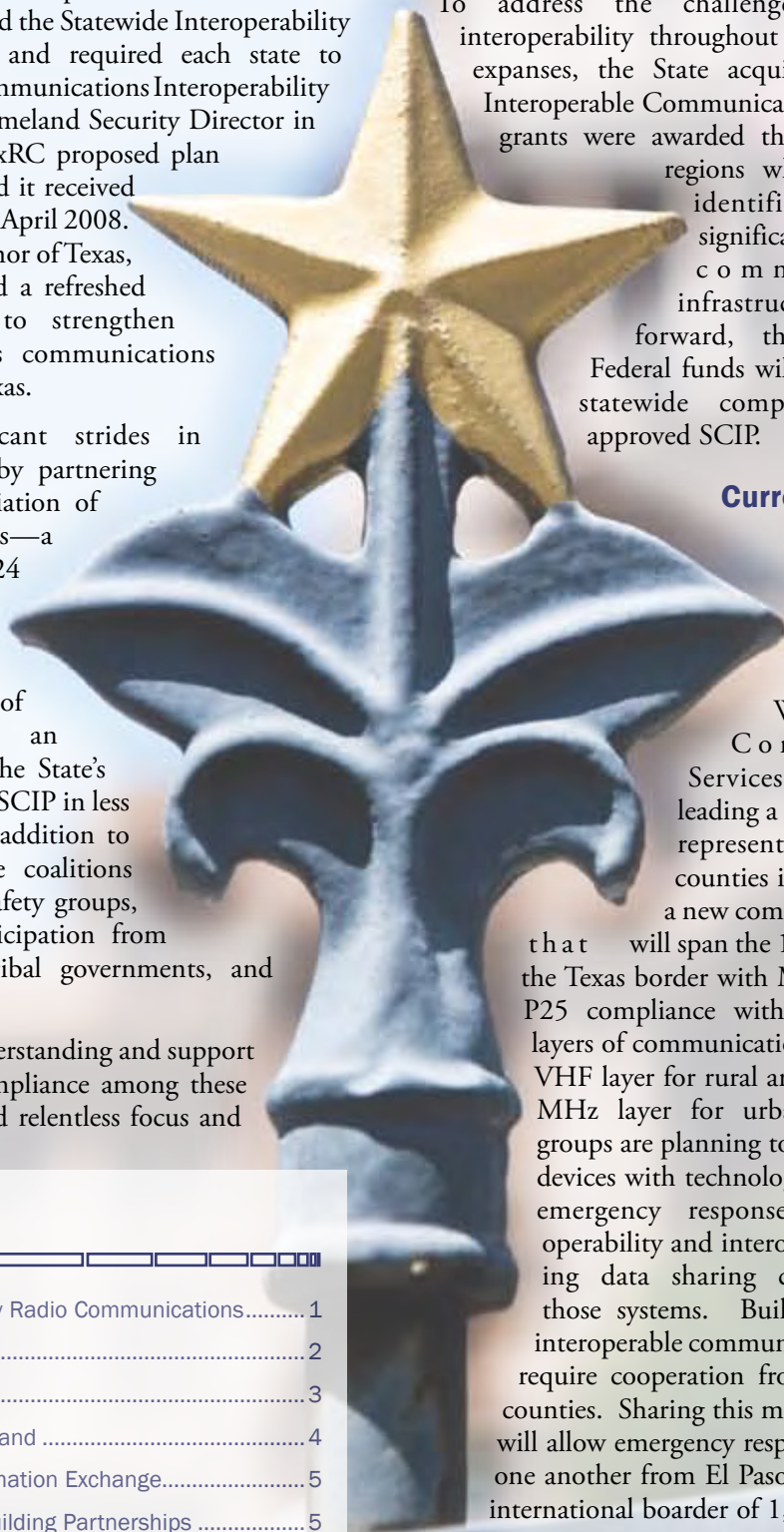
Texas leads the Nation in natural disaster declarations. The majority of these disasters occur along the Gulf of Mexico coastline from the international border with Mexico to the Louisiana State border. The Texas Coastal Communications Project is being organized in response to the multitude of disasters that take place along the coast. This project will bring together all coastal jurisdictions to address their emergency response needs on a consolidated level.

In September 2008, Hurricane Ike affected millions of Texas citizens, many of whom suffered great personal losses. Simpson participated firsthand in Hurricane Ike emergency response efforts and felt the effects of capability gaps present in the Texas Coastal Communications Project. “We need enhanced P25 communications systems to better handle weather events and help secure people and assets from potential terrorist threats. Our State has unique communications issues due to its geographic location,” Simpson said. He adds, “Successful implementation of the Texas Coastal Communications Project will significantly enhance our ability to improve communications in these areas.”

Currently, the 24 Texas regions are challenged with enhancing established governance committees to oversee the shared interoperable regional emergency radio communications systems, the Texas Border Communications Project, and the Texas Coastal Communications Project. Establishing rules of operation and a workable governance structure that will be useable by all practitioner groups are important issues that will require early planning and management.

### CONTENTS

|  |   |
|--|---|
| Texas to Improve Emergency Radio Communications..... | 1 |
| Director’s Message.....                              | 2 |
| Operation Golden Phoenix.....                        | 3 |
| Radio Over Wireless Broadband .....                  | 4 |
| SRFERS Enables New Information Exchange.....         | 5 |
| Focus Group Encourages Building Partnerships .....   | 5 |
| National Emergency Communications Plan .....         | 6 |
| In Your Own Words .....                              | 6 |
| Spotlight .....                                      | 7 |



## About Interoperability TECHNOLOGY Today

*Interoperability Technology Today* is published quarterly by the Science and Technology Directorate's Command, Control and Interoperability Division (CID) at no cost to subscribers. Its mission is to provide the emergency response community, policy makers, and local officials with information about interoperability initiatives nationwide, best practices, and lessons learned.

CID interoperability programs address both data and voice interoperability. CID is creating the capacity for increased levels of interoperability by developing tools, best practices, technologies, and methodologies that emergency response agencies can immediately put into effect. CID is also improving incident response and recovery by developing messaging standards that help emergency responders manage incidents and exchange information in real time.

Through a practitioner-driven approach, CID creates and deploys information resources—standards, frameworks, tools, and technologies—to enable seamless and secure interactions among homeland security stakeholders. With its Federal partners, CID is working to strengthen capabilities to communicate, share, visualize, analyze, and protect information.

**Subscriptions:** *Interoperability Technology Today* is available at no cost. If you are not currently on our mailing list, visit <http://www.safecomprogram.gov> to subscribe by clicking on the Contact Us link.

**Address Correction:** So that you do not miss an issue of *Interoperability Technology Today*, please notify us of any changes in address or point of contact. Visit <http://www.safecomprogram.gov> to update your contact information by clicking on the Contact Us link.

**Article Reproduction:** Unless otherwise indicated, all articles appearing in *Interoperability Technology Today* may be reproduced. However, a statement of attribution, such as, "This article was reproduced from the fall 2008 edition of *Interoperability Technology Today*, published by the U.S. Department of Homeland Security's Command, Control and Interoperability Division," should be included.

**Photo Credits:** Photos and graphics used in this edition of *Interoperability Technology Today* include iStock.com.

CID would like to acknowledge its practitioner-comprised Editorial Review Board for the valuable input it provided in reviewing article content for this edition.

**Disclaimer:** Contents of this newsletter do not necessarily reflect the opinions, views, or policies of the U.S. Department of Homeland Security; the Science and Technology Directorate; CID; nor the U.S. Government.



## UPCOMING EVENTS

### Events & Conferences

**Video Quality in Public Safety Conference**  
February 4-6, 2009  
Boulder, Colorado  
<http://www.its.blrdoc.gov/psvq>

**DHS S&T Stakeholders Conference West**  
February 23-26, 2009  
Bellevue, Washington  
<http://www.ndia.org>

**International Wireless Communications Expo**  
March 16-17, 2009  
Las Vegas, Nevada  
<http://iwceexpo.com/iwce2009/public/enter.aspx>



### DIRECTOR'S MESSAGE

By Dr. David Boyd

Entering its fifth year, the U.S. Department of Homeland Security's Office for Interoperability and Compatibility (OIC) remains committed to improving communications interoperability within the emergency response community. Three OIC initiatives in particular—the Multi-Band Radio (MBR), Voice over Internet Protocol (VoIP), and the Project 25 Compliance Assessment Program (P25 CAP)—reflect this commitment. Working closely with practitioners, each project tackles the multi-pronged issue of interoperability from a new angle. With demonstrated success this past year, the efforts of these three projects will continue to aid the emergency response community in 2009 and beyond.

#### Multi-Band Radio

For years, the emergency response community sought a single radio that could operate across all available public safety radio bands. Until recently, emergency response radios were limited to operating on a single radio band, which created challenges for the implementation of an MBR. However, with new spectrum in the 700 MHz and 800 MHz bands becoming available to public safety communications networks in February 2009, operating on an MBR is becoming more and more a reality.

After years of engineering, industry leaders finally focused efforts on developing a multi-band, multi-mode radio for the emergency response community. In February 2008, OIC partnered with Thales Communications, Inc. to develop and test a prototype of one such radio. Known as the MBR, this portable radio enables emergency responders to seamlessly communicate with partner agencies, regardless of the band in which they operate.

After making several updates to the prototype's software, OIC began conducting a series of laboratory tests to evaluate the radio's capabilities. Following the success of these laboratory environment tests, OIC will spend the bulk of 2009 extensively testing the MBR in the field. Plans include pilot demonstrations of the MBR in multiple regions across the Nation. These regions were selected for the diversity of emergency communications needs that they represent. During these pilots, Thales will provide agencies with the appropriate training and guidance to ensure they effectively employ the technology in their region. After the pilots conclude, evaluations from the user

community will be collected and used to further refine the MBR.

From these pilots, OIC will identify potential tools or accessories to develop for the general emergency response community. These tools or accessories will help emergency response leaders determine whether the MBR is right for their community and if so, how to best implement the technology. OIC will ensure this progressive technology continues to improve interoperability and communications during emergency response operations.

#### Voice over Internet Protocol

Voice over Internet Protocol, commonly referred to as VoIP, is a technology that has gained growing recognition in recent years. Capable of transmitting real-time voice services over IP-based networks such as the Internet, VoIP enables devices within a radio system's infrastructure to directly connect over any network. IP networks are notable for the flexibility they provide in call placement options, device addressing, and device placement. The combination of real-time voice communications with this increased level of flexibility results in a powerful tool for emergency responders. Despite the advantages of VoIP, manufacturers have not adopted a single standard; as a result, there is no guarantee that one manufacturer's VoIP devices will be able to interface with another's.

To address this issue, in 2006 OIC partnered with the National Institute of Standards and Technology's (NIST) Office of Law Enforcement Standards and the National Telecommunications and Information Administration's Institute for Telecommunication Sciences (ITS) to form a VoIP Working Group. Comprised of emergency response leaders and industry members, the Working Group establishes implementation profiles and best practice recommendations for VoIP interfaces. In 2008, the Working Group achieved a major success with its development of the Bridging Systems Interface (BSI) Core Profile. The BSI Core Profile defines the minimum standards, parameters, and values needed to enable voice interoperability between disparate VoIP-based radios. Tested and approved by the Working Group, manufacturers are now building VoIP-based equipment around this Profile. In 2008, the Working Group hosted two Plugfest sessions at which multiple vendors showcased their BSI-compliant



## Operation Golden Phoenix Brings Real-Time Emergency Scenarios to Training Events

In July 2008, Operation Golden Phoenix (OGP) hosted a series of coordinated response exercises that focused on all-hazards response, interoperable communications, information sharing, and tactical planning for man-made and natural disasters in San Diego, California. Members of the United States Marine Corps (USMC) Reserve Air Group developed the concept of OGP after Hurricane Katrina hit New Orleans, Louisiana—its principal focus centered upon improving the formal and informal relationships between military and civilian response entities.

Supported by the USMC, the first training session took place in 2007. OGP involved a series of information briefs and workshops designed to reinforce existing California State, Federal request, and assignment protocols; facilitate discussion regarding local incident management procedures; and, raise awareness of participating entities' resource capabilities. OGP training sessions simulated real-time emergency scenarios that incorporated 90 percent of factual components. Public safety groups, non-profit organizations, and private sector groups were invited to participate; both in 2007 and 2008, OGP training sessions brought together more than 800 diverse members of the emergency response community. These training sessions provided best practices and lessons learned—such as the need for continued interagency exposure and cooperation regarding incident management protocols—that apply to all levels of government and address interoperable obstacles facing rural and urban localities.

“One of the most important attributes of OGP is the way it provides a forum for the public sector to learn best practices of the private sector and vice versa,” says Kevin “Spanky” Kirsch, Director of the U.S. Department of Homeland Security's Science and Technology Directorate Office of Special Programs. “In addition, the main lesson we saw in play was that even the best technology can't benefit your agency if you don't prioritize interoperational capabilities with other agencies.”

George Bressler, Incident Management Coordinator for San Diego (California) Border Patrol and Federal Lead Planner for OGP, highlights the strengthened relationships that OGP training sessions produced for the represented regions. Bressler says, “We actively worked to coordinate non-traditional partners and heterogeneous traditional and non-traditional emergency response partners like police, fire, hospital, and military units with new technologies and tools in a manner that enhances resilient relationships. We found that OGP provided a unique opportunity for these groups to sit down and figure out how diverse training requirements and objectives can work together synergistically in a relatively low-cost no-fault environment.”

To achieve this environment of open discussion, OGP integrates three key elements into every training exercise: Communication, coordination, and cooperation. It is through these fundamental components of collaborative training that emergency groups develop core relationships. Establishing a healthy level of trust among diverse emergency response groups early and often supports efforts to improve interoperability nationwide.

To apply these three core components, OGP facilitated an emergency scenario at the port of Long Beach, California, in 2008. OGP 2008 implemented a full-scale training response to a maritime and land domain bio-terror attack scenario in Southern California with a satellite unmanned aerial systems component in Arizona. Emergency response groups—comprised of both classified and unclassified levels—used the event to evaluate which of their tools and technologies were interoperable once implemented. Bressler adds, “In addition to learning best practices, we were also able to see challenges that, should it have been a live emergency, we may not have been able to see.”

equipment. The success of the BSI Core Profile was reflected in the vendors' ability to seamlessly connect their devices with other vendors' equipment.

With a landmark year behind them, the VoIP Working Group will broaden its focus in 2009. Building on the BSI Core Profile, the group is developing a BSI Enhanced Profile that supports additional functions, such as the ability to transmit priority information, manage network information, and create secure links. This implementation profile will be used as the framework to address other application areas, such as the Wired End Unit to System interface or the Dispatch interface. The Group will also work closely with the user community to examine other ways that VoIP is being used by emergency responders. From these discussions, the Working Group will determine and prioritize the next interfaces addressed by implementation profiles.

### Project 25 Compliance Assessment Program

Project 25 (P25) aims to create a set of standards that will allow radios and other components to seamlessly interoperate, regardless of manufacturer. To ensure that technology being purchased by emergency responders is able to interoperate across manufacturers, OIC, NIST, and ITS partnered with industry representatives and emergency response leaders to form P25 CAP. P25 CAP is a voluntary program by which P25 equipment suppliers formally demonstrate their products' compliance with select P25 standards.

In 2008, P25 CAP officials gathered local, state, and Federal government officials to form the P25 CAP Governing Board. Meeting frequently, the Governing Board develops policies regarding various components of laboratory assessments that are being conducted under this program. These policies are used by laboratory assessment teams to evaluate and determine which laboratories are competent to perform P25 testing.

Once equipment is approved as P25 compliant, established laboratories will begin extensively assessing the equipment of manufacturers in 2009. As laboratories and manufacturers begin to compile the documentation developed as a result of the equipment assessments, P25 CAP leaders will work with equipment suppliers to collect and post all pertinent information on a public Web site. In addition, OIC will continue working with NIST to recognize additional laboratories and to ensure that existing laboratories remain competent to perform P25 tests. OIC's efforts will ensure that emergency responders continue to receive the best product for their needs.

### Looking to the Future

While there is no single interoperability solution that solves all communications problems, projects such as MBR, VoIP, and P25 CAP continue to advance us toward that ideal. Whether developing standards, piloting technologies, or evaluating equipment, each of these projects contributes to the ultimate goal of complete interoperability. Their work in 2009 will not only support emergency responders in the present, but will also influence the work of the future.



## Radio Over Wireless Broadband Technology Achieves Interoperability Milestone

Many people assume that emergency response agencies across the Nation are already interoperable and capable of sharing information in real time. In actuality, until now emergency responders could not talk to some parts of their own agencies—let alone communicate with agencies in neighboring cities, counties, or states. To successfully respond to day-to-day incidents and large-scale emergencies, emergency responders—police officers, fire fighters, and emergency medical services personnel—need to share vital data and voice information across disciplines and jurisdictions. With the creation of the Radio over Wireless Broadband (ROW-B) technology, emergency responders are now one step closer to communicating across previously disparate wireless radio and broadband communications systems.

### The Challenge

To exchange communications, emergency responders typically use wireless radio systems known as land mobile radios (LMRs) that are either hand-held or mounted in vehicles. With the evolution of technology, emergency responders are now gaining access to advanced communications capabilities, such as high-speed data transmissions—commonly known as broadband—and third generation wireless technologies. Since LMRs and broadband systems serve specific and different needs, they were not designed to communicate with each other. As a result, many agencies are forced to employ completely separate LMR systems and wireless broadband systems to accomplish their communications goals. The lack of interoperability between these two separate networks may compromise emergency response operations and endanger the lives of public citizens.

### ROW-B Technology

To address this capability gap, the Command, Control and Interoperability Division (CID) of the U.S. Department of Homeland Security launched the ROW-B project. In partnership with the National Institute of Standards and Technology (NIST), the Institute for Telecommunications Sciences, ISCO International, emergency response agencies, and industry partners, CID extensively researched how to connect existing LMR systems with new advanced wireless broadband technologies while leveraging the Geographic Information System (GIS) technology. This research yielded ROW-B—a technology by which emergency responders can communicate between traditional LMR systems and advanced wireless broadband communications systems while accessing location capabilities.

“ROW-B is extremely valuable in demonstrating the ability to bridge communications systems and tie communication and location together. The result is more intelligent and dynamic communications among emergency responders,” says CID Chief Technology Officer Luke Berndt.

The emergency response community has expressed an immediate need for this type of interoperable communications technology. In a 2007 National Public Safety Telecommunications Council questionnaire of more than 300,000 practitioners, respondents identified Push-to-Talk (PTT) and GIS as priority wireless broadband applications.

PTT over Cellular technology allows for walkie-talkie-type communication over a cellular phone network. This phone technology effectively allows a single user to reach multiple users through talk groups on a cellular network. By reducing the number of calls needed to coordinate a group, this technology saves critical response time. Integrating PTT over Cellular callers with LMR system users will significantly improve emergency response operations by allowing authorized, non-radio system users to communicate with response units.

GIS technology encompasses a host of technologies supporting location-based services such as location visuals of vehicles, equipment, resources, and other

emergency responders. The locations are displayed on maps that are generated in real time by GIS databases that contain important information such as roads, buildings, fire hydrants, and other geographic items that are of interest. These real-time maps provide emergency responders with vital information when they need it most.

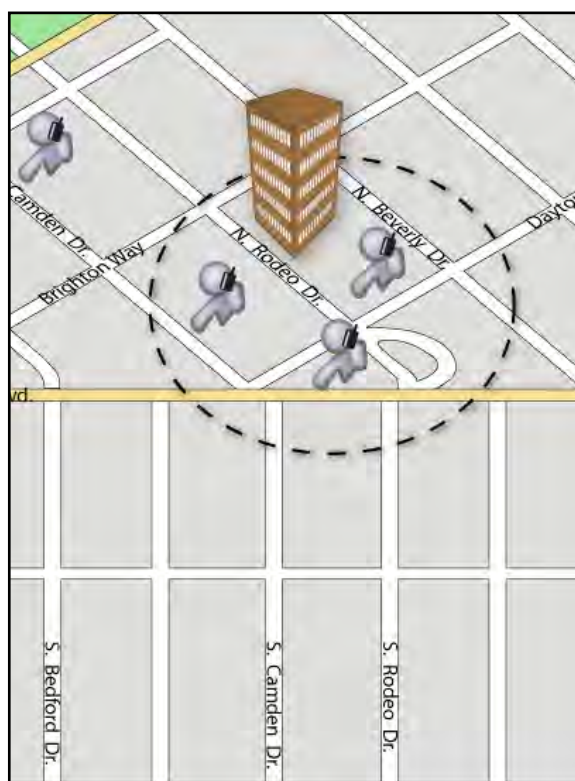
ROW-B places these important PTT and GIS broadband features into the hands of emergency responders.

As industry develops new technologies, it is critical that emergency response agencies are able to integrate them into current and future systems and operations. To link communications systems, emergency responders rely on connection points between systems known as bridging interfaces. To connect the LMR and broadband cellular systems, ROW-B uses an interface called the Bridging Systems Interface (BSI), which was developed in a joint effort between CID and NIST’s Office of Law Enforcement Standards (OLES). To demonstrate the impact of the BSI on interoperability and the integration of new broadband technology with existing systems, CID brought ROW-B to Washington, D.C.

### Washington, D.C. Pilot

A major milestone was reached in August 2008 when CID held the first pilot of the ROW-B technology in Washington, D.C. to demonstrate how to connect existing LMR systems with advanced broadband communications systems. In partnership with NIST OLES, the District of Columbia’s Office of the Chief Technology Officer (OCTO), and ISCO International, CID tested ROW-B in the first 700 MHz Broadband Network in the Nation.

“The ROW-B pilot represents an important milestone in our efforts to advance interoperability progress,”



Dynamic Talk Groups Based on Proximity

says CID Director Dr. David Boyd. “For the first time, we are breaking down barriers and broadening the circle of people who can talk in real time to significantly improve emergency response operations.”

Throughout July and August 2008, the ROW-B pilot connected OCTO’s existing LMR system with broadband devices and utilized GIS and PTT while using the BSI. This set-up allowed a single user to locate and communicate with multiple users through talk groups on the Washington, D.C. Regional Wide Broadband Network public safety 700 MHz high-speed network.

A kick-off event was held on Capitol Hill during which CID and its partners

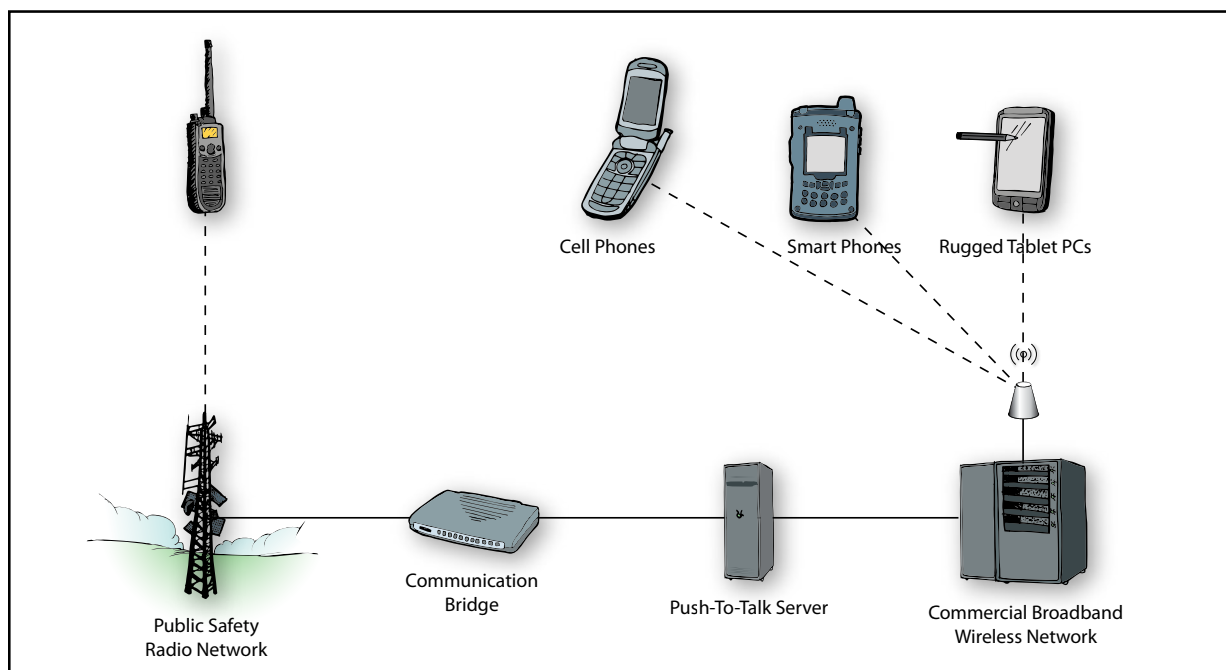
demonstrated the ROW-B technology for congressional members and staff, OCTO representatives, government agency officials, and media representatives. The event was widely covered in media outlets, including *Congressional Quarterly*, *Federal Times*, *Government Computer Week*, *Government Executive*, *Washington Times*, and numerous trade and online publications.

### Next Steps

ROW-B represents an important step toward improving interoperability nationwide. While addressing interoperability challenges from different angles, partners shared a common goal: to ensure that emergency responders nationwide can communicate with each other on demand.

“ISCO is honored to participate in the ROW-B pilot program,” says Chief Executive Officer Gordon Reichard. “The ROW-B pilot program has been instrumental in creating broadband, cellular, and WiFi-based technology that is properly focused on public safety needs.”

The impact of the ROW-B project reaches beyond technology. Presented with entirely new ways of communicating, emergency response agencies will now have an opportunity to create new standard operating procedures as well as new governance structures for managing incident communications. By documenting lessons learned and best practices from the ROW-B pilot, CID will be able to develop replicable tools, resources, and templates that will help agencies integrate existing and emerging communications systems.



ROW-B Research Project Overview

## SRFERS Enables New Information Exchange Capabilities across State Lines

An AMBER Alert comes up on a patrol car's scanner. It is for a missing child who is suspected of being abducted from a neighboring state. The officer submits a request for the suspect's photo and receives an image of the repeat offender within seconds. With this image, the officer will be able to apprehend the perpetrator more quickly and easily.

The State, Regional, and Federal Enterprise Retrieval System (SRFERS) is responsible for the success of this scenario. For the first time, criminal justice practitioners are able to exchange information—such as booking photos, driver license photos, corrections photos, and license plate data—in real time and across state lines. SRFERS is supported by the U.S. Department of Justice's (DOJ) National Institute of Justice (NIJ) and the U.S. Department of Homeland Security's (DHS) Command, Control and Interoperability Division.

Prior to SRFERS, this type of information was rarely shared across state borders. When exchanged, the written or verbal request was submitted to the specific agency and the report or photo—often of poor quality—would be faxed back to the requesting officer in days or even in a few weeks. DHS CID Program Manager Bruce Baicar says, "SRFERS enables criminal justice practitioners to operate as usual, but with the added ability to share photos and information across state lines. Prior to SRFERS, this type of information exchange may have taken an unspecified amount of time. Officers and investigators in the field are better equipped because of SRFERS." Imagine the case of the patrol unit searching for the suspect described in the AMBER Alert; if this officer did not have the suspect's photo on hand immediately, he may have missed an opportunity to locate the individual.

SRFERS provides users with privacy, policy, and technical standards as well as a suite of technology solutions. Combined, they provide a blueprint of technical building blocks, lessons learned, and best practices for law enforcement, corrections, and judicial agencies at the local, tribal, state, and Federal levels. Criminal justice and emergency response agencies are able to use these resources and technology solutions to leverage existing public safety infrastructure across the Nation.

To maximize integration and minimize cost, SRFERS relies on existing information infrastructures to demonstrate connectivity and exchange data in real time across state lines. Specifically, SRFERS uses networks such as the International Justice and Public Safety Information Sharing Network (Nlets), the Automated Regional Justice Information Sharing network, and established state networks. From these existing networks, SRFERS has created a toolkit to enable agencies to seamlessly share justice information. The toolkit consists of successful architectural models, technical specifications for open source messaging applications, transactions and scripts, templates for information sharing agreements, and technical and policy documentation guidance. The SRFERS toolkit serves as a central resource for criminal justice and emergency response personnel to access templates and standard documentation necessary for their investigations. Through multi-phase pilot demonstrations of the SRFERS toolkit, the project is extending information sharing capabilities to law enforcement agencies across the Nation.

SRFERS also uses the Global Justice Extensible Markup Language Data Model (Global JXDM). Regularly updated based on user input, the Global JXDM enables criminal justice personnel to exchange messages in a consistent manner. The Global JXDM provides criminal justice and emergency response agencies with an effective tool to share data and information on demand and in real time. Developed by the DOJ Office of Justice Programs in April 2003, the Global JXDM was specifically designed based upon the vocabulary and requirements necessary for criminal justice information exchange. Baicar says, "By incorporating the existing regional and state information exchange infrastructure, SRFERS has helped keep costs low and the transition to SRFERS applications simple. Because practitioners are already familiar with the program's set up, there has been little difficulty in adopting SRFERS."

From its inception, the SRFERS initiative has been driven by practitioner needs. Over time, technology and standards for communication and data exchange have developed with the input of users; as a result, criminal justice and public safety agencies nationwide have been able to acquire better tools for officers to complete their operations. At the same time, agencies across the Nation have been working to improve cross-agency and cross-jurisdiction information sharing on their own. Drawing on this wealth of knowledge and experience, SRFERS has incorporated input from local, state, and Federal practitioners into its framework.

In one instance, the SRFERS initiative adopted several elements of the DOJ Global Intelligence Working Group's National Criminal Intelligence Sharing Plan.

Drawing on the Plan's approach, SRFERS now uses information sharing systems already in place, develops standards to link disparate systems, develops operational requirements and technical specifications, develops resource guides and templates for agreements such as memorandums of understanding and standard operating procedures, and addresses legal and policy limitations related to the implementation of information sharing systems.

continued on page 8

## Focus Group Encourages Building Partnerships While Tackling Interoperability Obstacles

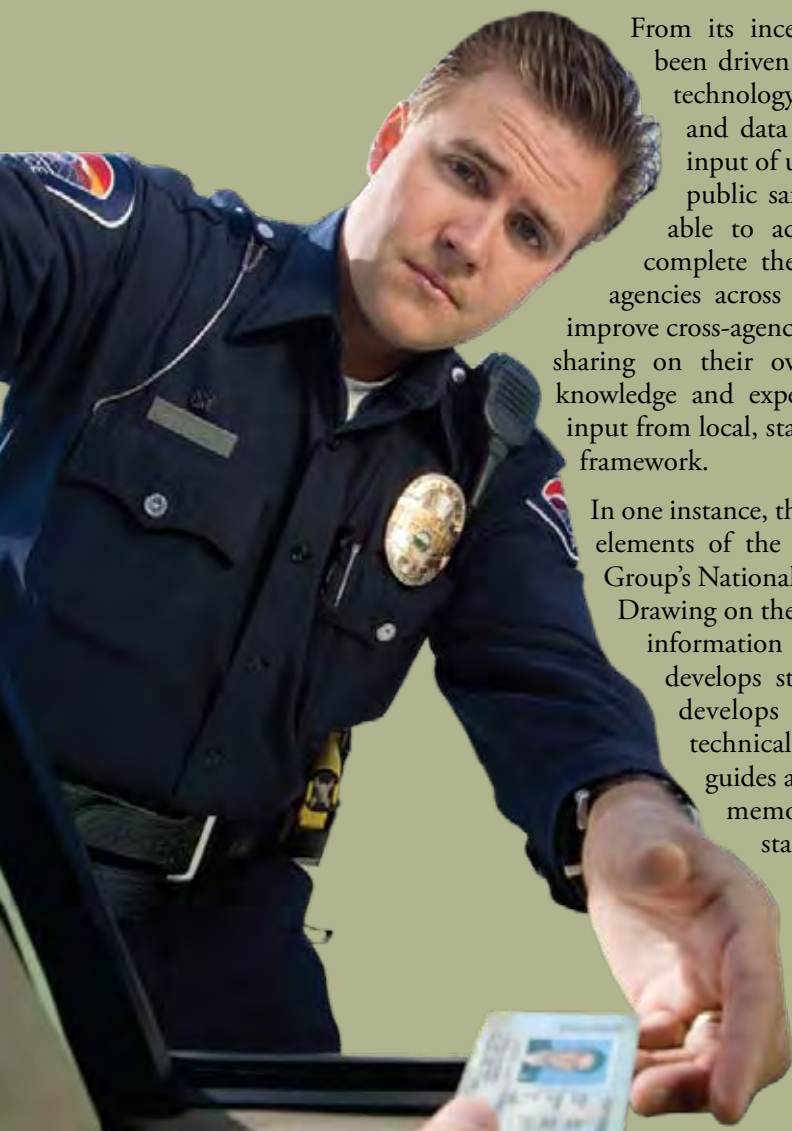
Emergency responders and representatives from the U.S. Department of Homeland Security (DHS), the National Guard, U.S. Northern Command, and other Federal homeland security agencies joined forces in Austin, Texas, for the Responder Interoperable Communications Focus Group (RICFG). The RICFG, initially held in the summer of 2008, served as a forum for participants to discuss obstacles and solutions to current voice interoperability issues. At the two-day summit, attendees participated in team-building exercises and discussed obstacles facing the emergency response community today—including technology, governance, funding, and operational issues.

Discussions at the RICFG emphasized the importance of establishing and improving cross-agency partnerships across local, tribal, state, and Federal agencies in order to enhance coordination, planning, and response. Attendees described common operational issues that arise during cross-border communications and how a coordinated communications response is impacted when Federal agencies are involved. Following these discussions, participants agreed that local, tribal, state, and Federal agency representatives must partner with DHS, the Department of Defense (DoD), and the National Guard to enhance our Nation's coordinated interoperable communications abilities. Lastly, attendees participated in a session that focused on next steps for a joint DHS-DoD-National Guard interoperable communications effort.

In addition to the discussions and action items developed at the RICFG, the event encouraged face-to-face networking among emergency response groups and building partnerships across a diverse community. Representatives from California, Delaware, Oregon, Texas, Washington, and Washington, D.C. met to actively practice collaboration among various agencies.

Formal and informal discussions revealed a general consensus that technology was not a major impediment to achieving interoperable communications. Instead, participants found that in most cases, interoperability problems stemmed from governance, collaboration, training, exercises, and standard operating procedures issues. Participants agreed that these areas must be addressed if all involved parties wish to establish seamless communications among government agencies and military entities.

The RICFG was organized and sponsored by the DHS Science and Technology Directorate's TechSolutions program. This program provides funding for near-production technology solutions that address mission capability gaps identified by the emergency response community. After a review process, TechSolutions funds selected advanced technologies that meet 80 percent of the operational requirements identified by emergency responders; each project will receive no more than \$1 million for a 12-15-month time frame. In the hands of emergency responders, the TechSolutions technologies will enhance a variety of operations by filling capability gaps. Planning is currently underway to hold another RICFG to continue this collaborative forum among government and practitioner partners.





## National Emergency Communications Plan Positions Emergency Groups for Interoperability Success

The U.S. Department of Homeland Security (DHS) achieved a major interoperability milestone upon releasing the National Emergency Communications Plan (NECP). The NECP outlines recommendations and measurable goals for local, tribal, state, and Federal agencies to establish minimum levels of interoperability. It is the first formal plan to provide all levels of government with a shared strategy to improve emergency communications for both urban and rural localities. This unified plan focuses on improving interoperability among all levels of government and across all disciplines through five main categories: Governance, planning, technology, training and exercises, and disaster communications capabilities. Paired with other Federal departments' strategies and state plans, the goals of the NECP—when accomplished—will enhance emergency response efforts across the Nation, including command and control procedures.

The DHS Office of Emergency Communications (OEC) laid the groundwork for the NECP by supporting the development of Statewide Communication Interoperability Plans (SCIPs). Through the SCIP development process, every U.S. State and territory developed scalable goals that aim to improve and measure interoperability-based progress. The 56 SCIPs require the involvement of emergency response practitioners from every level of government throughout the implementation process. Once implemented, the

SCIPs will establish a minimum level of interoperability and emergency preparation awareness among emergency responders. Building on the work of the SCIPs, the NECP provides practitioners with a shared strategy to address communications challenges that may arise during day-to-day emergencies and large-scale disasters.

The NECP addresses this challenge of moving our Nation toward the end goal of cross-jurisdictional emergency preparedness. The NECP represents the Nation's first strategic plan to improve emergency response communications and preparedness, and complements overarching homeland security and emergency communications legislation, strategies, and initiatives—including the SCIPs. To move the Nation toward the goals of the NECP, the plan lays out recommended milestones that cut across disciplines and jurisdictions. Therefore, the NECP's successful implementation relies on partnerships and a commitment from a variety of stakeholders to work together to achieve the plan's vision: that emergency response personnel can communicate at all

levels of government, across disciplines, as needed, on demand, and as authorized.

Chief Charles Werner, Charlottesville (Virginia) Fire Department and chairman of the DHS SAFECOM Executive Committee, explains how the NECP provides the opportunity for emergency response agencies at all levels to work together to effectively implement the plan. "This plan differentiates itself from other public safety preparedness initiatives in the way it prioritizes the engagement of emergency response practitioners at all levels and provides agencies with goals to accompany the specified recommendations," he says.

### The Road Ahead

Moving forward, the NECP outlines specific goals for emergency responders spanning the next five years. Supported by the NECP and indicated in the Urban Area Security Initiative (UASI)—an initiative outlining resources for the specific equipment, planning, and training and exercise needs of high threat urban areas—by 2010, 90 percent of high-risk inner city and urban regions will require no more than one hour to respond to day-to-day incidents that involve multiple agencies and jurisdictions.

**continued on page 8**



### IN YOUR OWN WORDS

By Timothy Loewenstein, Buffalo County (NE) Supervisor

## The Interoperability Solution: People, Not Technology

Throughout the last several years, the subject of interoperable communications has increasingly become a nationwide concern among citizens and Federal leaders. With the release of the National Emergency Communications Plan and the growing number of Federal and public groups lobbying for interoperable emergency response communications, the public has become more and more familiar with the need for improved communications among emergency responders. In the process of communicating the need for interoperable communications, however, a critical aspect of the solution has not been fully grasped. While citizens understand the need, they do not fully understand the root cause of interoperability problems. Just as emergency responders have done in the past, the general public often attributes all interoperability problems to technology.

Admittedly, technology solutions that connect public safety officials across disciplines and levels of government comprise a critical component in improving interoperability nationwide. It is important to note that advanced devices and methodologies alone cannot fix the problem. The real solution lies in the relationships of people, not technology. Emergency responders who embrace interoperability as a priority and demonstrate a willingness to adopt new communications practices will foster an environment in which interoperable technologies can be optimized to their fullest extent.

The entirety of my professional career has centered upon communications. As a volunteer with local fire and sheriff departments and as chairman of various law committees, I have witnessed the failures and successes of communications in emergency response operations. Repeatedly, I see that the use of a "we" mentality is more effective than an "I" mentality. As an agency seeks to incorporate interoperability practices into their everyday routine, it is helpful to ask, "How can we collaboratively accomplish this goal?"

For example, a common challenge on the path to achieving interoperability is establishing or implementing plain language. I have seen firsthand that agencies from other regions do not understand the acronyms used by my own region's units. This raises the question: Even if multiple regions have a singular radio system, how do they intercommunicate so that they understand one another's terminology? It is the human element—not a technology solution—that is needed to resolve the problem here. Fostering a willing attitude among emergency response groups to cooperate and establish a common language will achieve a heightened level of interoperability.

In addition to the advantage created by emergency response groups prioritizing the use of plain language, emergency response groups must incorporate both technology and the "we" mentality of cooperation into their day-to-day standard protocols. Available interoperable tools must become integrated into the typical daily routines of emergency response groups across the Nation. When these tools are used on an everyday basis, emergency responders are better positioned to implement interoperability practices when disasters or incidents occur. Emergency responders should aim to work together in non-critical situations and cooperative environments that promote the use of all assets both technological and human.

Ultimately, the fundamental solution to address interoperability challenges: Establish trust! Agencies need to recognize that on the scene of an emergency, their work will not be compromised by exercising a "we" mentality; rather, it will be enhanced. Interoperability progress will develop quickly and soundly when members of the emergency response community understand that we are stronger together than we are individually.

Throughout his career, Tom Sorley, Deputy Director of Radio Communication Services for the City of Houston, Texas, has worked tirelessly to solve public safety telecommunications issues. An advocate and administrator for more than 22 years, he began his career with the Orlando (Florida) Police Department 9-1-1 Center and now serves in the Nation's fourth largest city: Houston, Texas. An alumnus of the Southern Police Institute Command Officer Development Course, Mr. Sorley holds a Bachelor's degree in management and a Master's degree in business. He has been awarded numerous certificates recognizing his efforts to aid interoperability progress across regions.

Mr. Sorley is regarded as an expert in local and state emergency communications issues. In addition to his work as the Communications Manager for the Orlando Police Department and Orange County, Florida, he has also acted as Chairman for multiple industry committees at many levels of government, including the Association of Public Safety Communications Officials and the National Public Safety Telecommunications Council (NPSTC). He is currently the acting Chairman of NPSTC's Technology Committee and Vice Chairman of the Project 25 Compliance Assessment Program's Governing Board.



## Q&A with Tom Sorley

**Q: In your professional career, how did bridging the interoperability gap become a focus for you?**

A: I have spent the vast majority of my career—first in police dispatch and now as a member of local and national public safety communications boards—working to establish more effective interoperable communications among emergency responders. It was in those initial years in the Orlando Police Department that I realized the problem of interoperability was far more extensive than I had originally thought. This became starkly clear to me when Orlando hosted the World Cup in 1994. It was amazing to witness an event that required assistance from so many different agencies. Unfortunately, several units from different jurisdictions were unable to talk with one another, which posed several obstacles in our efforts to effectively secure the event.

**Q: What interoperability-related challenges have you found to be the most significant for those emergency responders serving on the front lines?**

A: My answer here is two-fold: One challenge is helping various emergency responders identify interoperability as a critical need for their unit. With the wide coverage of recent large-scale emergencies such as September 11, 2001, and Hurricane Katrina, interoperability has been thrust into the national spotlight. As a result, the public and the Federal Government have devoted increasing attention to the importance of interoperability. Until this recent transformation in the public eye, it was difficult to achieve buy-in with emergency responders. It proved particularly challenging in rural regions where agency officials did not see the necessity of interoperability in day-to-day

incidents. Meanwhile, in a large city like Houston, not all emergency response networks perceived the need for interoperability either. Since large agencies often use more complex and expansive wireless communications, they may not perceive the obstacles facing smaller agencies with limited communications capabilities. There are a separate set of challenges for rural and metropolitan regions, but all of the challenges are equally significant. While many agencies nationwide can now exchange information across jurisdictions, not all emergency responders know the measures that are taken to achieve this level of interoperability. If an organization doesn't recognize the need for interoperability, then they will not likely spend extra funds on interoperability-based technology or initiatives.

Secondly, despite common belief, technology issues are not holding back emergency response communities from making interoperability progress—the culprit is actually what we call “turf issues.” Emergency response agencies tend to lack flexibility in establishing a common language that can be used across disciplines and jurisdictions for every level of emergency. Groups want to keep the language they've used for years instead of adopting new terms used by other units. It can, however, be done. California is an example of a state that has worked diligently for several years to develop interoperable language and methodologies that are successfully used by emergency responders across regions.

**Q: What type of emergency-based communications progress would you like to see rural and urban regions make in the coming years?**

A: Over the last 10 years, the emergency response community has been moving toward standards-based communications, such as universal broadband data communications or standards approved by the Project 25 Compliance Assessment Program. Currently, there are serious plans in the works for a wireless communications network that will span the entire Nation. If we can bring this network into fruition, then public safety groups on all levels in rural and urban regions will be able to meet voice communications system requirements through a data network more easily.

**Q: What has been the most rewarding accomplishment you have seen thus far in your work to better establish interoperability throughout the emergency response community?**

A: In Orange County, Florida, I had the opportunity to serve as Chairman for a regional communications committee. The committee petitioned for a grant that provided funding for a nine-county regional interoperable overlay. This overlay was designed to address a critical component involved in achieving interoperability: Establishing a key infrastructure that allows responders to travel from place to place and maintain communication with a hand-held radio. This type of infrastructure makes it possible for people to communicate without having to transport, set up, or activate any other equipment. The overlay in the Orange County region brought interoperable capabilities to counties that had been unable to seamlessly communicate and successfully exchange information in the past.

#### SRFERS from page 5

SRFERS began as a DOJ NIJ grant program with the goal of developing interstate criminal justice and emergency response information sharing for the Pacific region of the United States. The first phase resulted in three proof-of-concept prototypes that enabled emergency responders to share photographs, license plate data, and Nlets information across state lines. During the initial phase, SRFERS also developed technical specifications for the exchange of driver license images. Now in phase two and with the support of additional Federal partners, SRFERS is expanding upon the developed prototypes and resources. As a result, more agencies are able to share the same type of information across more states.

SRFERS has developed a more effective information sharing system for the emergency response community and effectively improved practitioner access to information across state boundaries. Now equipped with the ability to share new types of information across state lines in real time, criminal justice officials have an advantage in completing their daily operations. This capability enables increased case clearance and fewer perpetrators on the street. Through the suite of technology solutions and toolkit of templates and resources, SRFERS is proving critical to enhancing the safety of communities and the effectiveness of law enforcement, judicial, and correctional agencies across the Nation.

#### NECP from page 6

By 2011, 75 percent of non-UASI regions are slated to achieve the same level of emergency communications response. By 2013, 75 percent of all jurisdictions will be able to demonstrate response-level emergency communications specified by the NECP within three hours of a significant event.

“The NECP marks the first time that a national plan has outlined emergency communications goals for urban and rural agencies, Federal Government divisions and private organizations, and emergency response groups of any discipline. This will serve as an invaluable tool that can align the mission and formal action plans of emergency response groups nationwide,” says Chief Werner.

#### Many Objectives, One Goal

The NECP is comprised of seven objectives—Objective 4 of the NECP, Standards and Emerging Communications Technologies, recognizes the benefits of advanced broadband services and proposes solutions to spur the deployment of emerging communication technologies. The NECP seeks to achieve this end goal by defining national milestones for its public and private sector stakeholders, including accelerating the development of voluntary consensus standards for existing and emerging technologies. DHS’s Office for Interoperability and Compatibility plays an important role in the implementation of the NECP in this regard and will continue its strong partnership with OEC on technology and standards issues.

*To read the full length NECP, visit [http://www.dhs.gov/xlibrary/assets/national\\_emergency\\_communications\\_plan.pdf](http://www.dhs.gov/xlibrary/assets/national_emergency_communications_plan.pdf).*

# Interoperability TECHNOLOGY Today



Homeland  
Security

**A Resource For the Emergency Response Community**

Winter edition 2009

**“This edition features ...”**

- Texas to Improve Emergency Radio Communications
- Operation Golden Phoenix Training Session 2008
- Radio Over Wireless Broadband Achieves Milestone
- SRFERS Expands Information Exchange Capabilities
- Responder Interoperable Communications Focus Group Builds Partnerships
- National Emergency Communications Plan Provides Measurable Goals
- Spotlight on Tom Sorley

Command, Control and Interoperability Division  
Science and Technology Directorate  
U.S. Department of Homeland Security  
Washington, DC 20528

PRESORTED STANDARD  
U.S. POSTAGE PAID  
ANNAPOLIS JUNCTION, MD  
PERMIT NO. 2538