



# Interoperability TECHNOLOGY Today

A Resource For the Emergency Response Community

Summer 2009



## Interoperability Infiltrates Georgia's Emergency Response Agencies

Since 1976, the State of Georgia has conducted six statewide assessments of public safety communications. Among the emergency response issues that were identified in each assessment, one remained a constant: interoperable communications. In the most recent survey—conducted in 2004—emergency responders identified communications interoperability as the most important issue responders faced. Georgia Emergency Management Agency (GEMA) Terrorism, Emergency Response and Preparedness Division Director Ralph Reichert says, “We were surprised to find the number one priority statewide was interoperable communications. That pounded into our brains, and we decided we needed to address this issue.” Drawing on funding from the State’s Homeland Security Grant funds, GEMA officials set out to find a statewide interoperable solution.

As State officials began exploring the issue, it became clear that there were several obstacles to implementing a statewide interoperability solution. Even with the support of U.S. Department of Homeland Security, funding remained an issue. Previous forays into interoperability solutions had yielded expensive technologies that surpassed the \$200 million mark. In addition to cost-related issues, the size and scope of the undertaking proved a challenge.

With 159 rural and urban counties in the State, agencies already possessed a wide range of communications systems that operated on multiple radio frequencies. Therefore, any system developed would have to accommodate the various needs of agencies and their systems across the State. With these criteria in mind, GEMA partnered with the Georgia Tech Research Institute (GTRI) to identify, develop, and implement an appropriate solution.

When researching various solutions, GTRI targeted affordable systems that would be less intrusive and easier to implement. GTRI Principal Research Associate Leigh McCook explains, “What we didn’t want to do was place a burden on the local jurisdictions.” To ensure that the voices of local responders were being heard, GTRI employed a bottom-up, practitioner-based approach.

Cognizant of the needs of local emergency response agencies, GTRI avoided solutions that would replace existing technologies or add another radio to responders’ belts. These approaches exceeded the available resources and threatened the daily operations of local agencies, which did not have the funding or manpower to transition to and train on new systems. Instead, GTRI explored options that built on the existing infrastructure. They eventually developed the Georgia Interoperability Network (GIN)—a gateway system that builds on existing radio frequency infrastructure, such as the Internet Protocol network, without expanding the radio footprint.

The GIN implements a public safety answering point (PSAP) at 9-1-1 dispatch centers in each of the participating regions. The PSAPs display incoming calls as icons on the dispatch computers, which dispatchers can select to connect calls from users throughout the State. The GIN can patch calls across all frequencies and devices used by participating law enforcement, fire, and emergency medical service agencies in the State.

With a price tag of only \$8 million, the GIN has proved to be an affordable solution. The State has been able to fully fund the Network—effectively avoiding local funding issues. Despite the relatively low cost of the system, State officials opted to implement the GIN in phases to spread out the cost of a one-time statewide implementation. Over the course of five years, the GIN has been implemented in 141 counties across the State. Each implementation is tailored to the needs and capabilities of the region.

continued on page 6

### CONTENTS

Georgia's Emergency Response Agencies .....	1
Director's Message.....	2
Information Sharing and Virtual USA.....	3
Laboratories to Test Project 25 Radio Equipment.....	4
GPS Technology Connects Emergency Responders .....	5
In Your Own Words .....	6
Spotlight .....	7
Open Information Sharing Network.....	8



## 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 and Liz Kennedy.

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

**Association of Public-Safety Communications Officials**  
August 16-20, 2009  
Las Vegas, Nevada  
<http://www.apco911.org/new/conference>

**International Association of Fire Chiefs**  
August 27-28, 2009  
Dallas, Texas  
<http://www.iafc.org>

**International Association of Chiefs of Police**  
October 3-7, 2009  
Denver, Colorado  
<http://www.theiafp.org>



### DIRECTOR'S MESSAGE

By Dr. David Boyd

Imagine it is September 2010, and you are a Louisiana emergency responder bracing for a Category 5 hurricane. Louisiana activates the State emergency operations plan and opens the Virtual Louisiana Portal to neighboring states and to the Federal Emergency Management Agency's Region VI Incident Management Center, which immediately alerts the National Operations Center (NOC). Louisiana's neighboring states do the same. Opening their portals to one another and to the NOC creates a regional common operating platform (COP) that will enable coordinated response and recovery efforts.

Almost immediately, your agency begins to work with homeland security practitioners across the region—including local, tribal, state, and Federal emergency response practitioners; the National Guard; the private sector; non-governmental organizations; and faith-based organizations. Together, you begin coordinating preparations for response and recovery to the hurricane, including planning for mass evacuations and supplying food, medical resources, and other assistance. Using the regional COP, you and your fellow practitioners are able to track the hurricane and pre-position assets to assist in the response efforts. While this is occurring, the President, state officials, and homeland security practitioners alert the public using the Commercial Mobile Alert System (expected to be fully operational in September 2010) to geographically target cell phones, personal digital assistants, billboards, and other devices.

Meanwhile, officials from the surrounding areas and the Federal Government use multi-band radios that adapt to local frequencies and protocols. Using these radios, you are able to communicate not only with emergency response agencies, but also with local officials and non-governmental and faith-based organizations that traditionally provide support in large-scale emergency situations. Those stakeholders without radios use their laptops or cell phones to interface with the radio networks. Meanwhile, homeland security practitioners in the field use a variety of mobile platforms, including "smartphones" as well as compact, rugged wireless computers to "see" what the command center can see. Video feed and maps are updated in real time so practitioners have the information they need—and only what they need—as the storm makes landfall. In short, decision makers and practitioners in the field, including you, are able to access what was not available during Hurricane Katrina: critical information.

Unfortunately, this scenario is only a vision of what could be. Today, very few practitioners have a shared

COP or other tools to address the full spectrum of information acquisition, management, analysis, sharing, and security issues associated with a full operational response. The Command, Control and Interoperability Division (CID) within the U.S. Department of Homeland Security (DHS) is working to meet this need through the Virtual USA Initiative.

### Virtual City, State, Regional, and Federal Initiatives

The Virtual USA Initiative builds upon a number of initiatives that have been undertaken at the local, state, regional, and Federal levels to address these issues. At the state level, Virginia and Alabama are using standards-based, open architecture geospatial technologies to create statewide systems known as the Virginia Interoperability Picture for Emergency Response and Virtual Alabama, respectively. As COPs for emergency response, these systems are capable of seamlessly integrating hundreds of previously disparate data sets. States such as Louisiana and Mississippi are engaged in similar efforts. The City of Beverly Hills, California, has also embarked on a multi-jurisdictional initiative to launch a platform that can be shared by partners from across California.

At the Federal level, the DHS Office of Infrastructure Protection has established DHS Earth to provide key elements of a common operating picture. In addition, there are a number of other initiatives, such as the United Incident Command Decision Support, that employ standards to enable the sharing of disparate data sets—such as the information in computer-aided dispatch systems—and make them available to all operations platforms.

Looking forward, the DHS Science and Technology (S&T) Directorate is leading the Regional Operations Platform Pilot (ROPP), which will bring together several states—Alabama, Florida, Kentucky, Mississippi, Tennessee, Texas, and Virginia, as well as observers from Georgia—to create an enhanced regional version of the Virtual Alabama and Voice Interoperability for Emergency Responders concepts. ROPP integrates existing platforms, enhanced visualization tools, and other data sets to allow participating states' systems to interoperate and exchange data with each other, regardless of the particular platform or application in use.

### Virtual USA

While these efforts represent important progress in addressing the problem, the Nation's ability to seamlessly share information across localities, states,

# Information Sharing and Virtual USA

The need for real-time, actionable information is critical during both day-to-day incidents and emergency response operations. Therefore, to make information accessible to emergency responders as needed, regardless of time, location, or operating system, the Command, Control and Interoperability Division (CID) within the U.S. Department of Homeland Security created Virtual USA. Through this Initiative, CID and the DHS First Responder Technologies program are partnering with local, tribal, state, and Federal agencies to build on the shift away from proprietary systems. Virtual USA aims to enable technologies to connect more easily across disciplines and jurisdictions; thereby improving emergency response operations.

Just a few examples of CID's efforts in support of Virtual USA's information-sharing initiatives include AZLink, the Critical Infrastructure Inspection Management System (CIIMS), and the Regional Information Sharing and Collaboration (RISC) program.

## AZLink

Funded by CID, AZLink allows law enforcement officers in Arizona to use personal digital assistants to access information—including criminal histories, mug shots, driver license data, and incident reports—that they traditionally need a computer system to access. Officers are also using the technology to access maps and aerial photographs to assist in investigations. AZLink has expanded from a pilot project originally in southern Arizona to an initiative involving agencies across the State as well as the Arizona Counter Terrorism Information Center.

## Critical Infrastructure Inspection Management System

First implemented by the Maryland State Police, CIIMS provides an efficient, cost-effective way for emergency responders to manage inspections of critical structures such as dams, bridges, and large industrial complexes. CIIMS enables state law enforcement officers to complete inspections by air quickly and efficiently with an easy-to-use, tablet-sized computer known as an electronic flight bag (EFB). Equipped with touch-screen controls that aid data collection efforts and expedite information sharing among local, state, and Federal intelligence communities, the EFB gathers inspection information, which can then be downloaded into a common database. CIIMS helps prioritize inspections based on input from local, state, and Federal agencies and industry. The Los Angeles Police Department used the technology for security at the 2009 Academy Awards, expanding the scope of CIIMS's use from the air to include the ground.

## Regional Information Sharing and Collaboration

Through the RISC program, CID is developing enhanced information sharing capabilities critical to improving the capacity of law enforcement and other emergency response agencies to protect the American public against terrorism and other criminal acts. Emergency responders in local, tribal, and state law enforcement and emergency response agencies are in critical need of inter-agency and inter-regional information sharing technology implementations. To address this need, RISC provides a user-driven research and test capability to address threat dissemination and information sharing requirements through rapid prototyping, experimentation, and operational demonstrations of new processes and applications.



and regions is still limited, and current strategies to resolve information sharing issues are fragmented. Through the Virtual USA Initiative, CID and the DHS First Responder Technologies program are partnering with local, tribal, state, and Federal agencies to build on the shift away from proprietary, stove-piped systems toward standards-based, commodity-driven, open architecture technologies. This shift from proprietary systems allows technologies to connect more easily across disciplines and jurisdictions for emergency response operations.

Since many communities have significant resources invested in legacy platforms that they cannot afford to abandon, Virtual USA leverages a system of systems approach to seamlessly share relevant information when needed. More specifically, it aims to foster the integration of disparate technologies across the information management lifecycle—linking tools used for the collection, analysis, management, communication, and protection of actionable data—both within each and across components.

Drawing on the experiences of Virtual City, Virtual State, Virtual Region, and other CID and DHS S&T programs, Virtual USA will demonstrate and share lessons learned and best practices with local, state, and regional jurisdictions.

## The Virtual USA Initiative

- **Integrates Existing Frameworks:** Virtual USA integrates a set of processes and solutions that complements existing policies, processes, and architectures in each of the respective states. It aims to establish seamless information exchange among participants, as needed and as authorized.
- **Builds on Existing Investments:** Significant resources have already been expended on information sharing platforms, architectures, viewers, radios, and other solutions. Virtual USA does not seek to replace these systems, but instead leverages a system of systems model to permit both new and existing technologies and concepts to exchange information.
- **Draws on Practitioner Input:** Virtual USA was created based on the needs of local, tribal, and state practitioners to manage data access within their own jurisdictions and to share information with relevant jurisdictions across the Nation, when needed. Virtual USA will continue to include practitioners in every step of the process.
- **Employs a Comprehensive Approach:** Virtual USA is not limited to making information exchanges possible between only two agencies or fixed points; instead, the initiative will foster dynamic information sharing among all relevant practitioners.

As we look to the future, CID will dedicate efforts to provide you, the homeland security practitioner, with a toolkit that includes the essential technologies, expertise, and processes to acquire, manage, analyze, share, and secure information. Several projects within CID—including the Critical Infrastructure Inspection Management System, the Multi-Band Radio project, and Emergency Data Exchange Language data messaging standards—will develop aspects of the toolkit to support the Virtual USA Initiative. Additional information about select Virtual USA projects can be found in the sidebar, “Information Sharing and Virtual USA,” on page 3. Leveraging CID's toolkit, homeland security practitioners across the Nation will be able to seamlessly share information as appropriate and when authorized.

## Laboratories Approved to Test Project 25 Radio Equipment

The U.S. Department of Homeland Security's (DHS) Office for Interoperability and Compatibility (OIC), along with the National Institute of Standards and Technology (NIST), is proud to announce that the first set of laboratories has been approved to test Project 25 (P25) radio equipment. This is a major milestone in OIC's quest to improve interoperability for emergency responders.

OIC is granting recognition to eight laboratories, thus enabling P25 manufacturers to test their equipment and provide Suppliers Declarations of Compliance (SDoCs) for P25 interoperable technologies. "A number of people from government and the private sector have been working very hard over the last two years to make the P25 Compliance Assessment Program a reality," comments Dereck Orr, Program Manager for Public Safety Communications in NIST's Office of Law Enforcement Standards.

"For the first time, we have a group of formally recognized laboratories that have openly proven their competence at performing P25 testing. This will provide added confidence to the user community that the equipment they are buying performs to the P25 standards," Orr continues. Laboratory recognition is a requirement of the P25 Compliance Assessment Program (P25 CAP)—a DHS initiative launched in 2006. A list of recognized labs can be found at <http://www.safecomprogram.gov>.

Among others, emergency response interoperability challenges facing our country were highlighted once again by the tragic events of September 11, 2001, and Hurricane Katrina. These events highlighted the need for responders to communicate and share information seamlessly across disciplines and jurisdictions to successfully respond to day-to-day incidents and large-scale emergencies. Currently, most practitioners cannot communicate with members of their own agencies, let alone with responders in other cities, counties, and states. Multiple products and applications have been developed to support and improve radio communications and its associated infrastructure; yet, because manufacturers use different technical approaches, these products are often incompatible.

In 1989, P25 was launched to develop standards that allow radios and other components to interoperate regardless of manufacturer. The goal of P25 is to specify formal standards for interfaces between the various components of a land mobile radio system, which is commonly used by emergency responders in portable handheld and mobile vehicle-mounted devices. Despite the advantages of this system of standards, there was not a process in place to confirm that equipment advertised as P25-compliant actually met all the criteria.

In response to this discrepancy, Congress passed legislation calling for the creation of the P25 CAP. The P25 CAP is a partnership of OIC, NIST, industry, and the emergency response community. A P25 CAP Governing Board comprised of local, state, and Federal government representatives establishes the policies of the P25 CAP and assists in the administration of the program. The P25 CAP will provide the more than 60,000 emergency response agencies nationwide with a consistent and traceable method to gather P25 compliance information on the products they buy.

"The P25 CAP lab approval process will better inform the emergency response community and allow agencies to procure equipment with an increased confidence that it complies with P25 standards," Luke Berndt, OIC Chief Technology Officer says.

Before any equipment can be tested, the P25 CAP requires test laboratories to demonstrate their competence through a rigorous and objective assessment process based on internationally accepted standards. Becoming a recognized laboratory is voluntary. To initiate the laboratory recognition process, a laboratory must first submit an application and a copy of their quality manual. The application

and quality manual will then be reviewed by a laboratory assessment team assembled by the P25 Laboratory Program Manager. If the laboratory assessment team finds any non-conformities with the documentation, these issues may be addressed prior to the on-site assessment. During the on-site assessment, the laboratory assessment team may examine equipment, facilities, test reports, and the management system; observe demonstrations of testing; review quality and technical records and procedures; and review the biographies of staff to determine their competency in their particular area of expertise. An on-site assessment is conducted as part of the initial recognition and, at minimum, every three years thereafter. Laboratories may require more frequent assessments as new standards and interfaces are included in the P25 CAP. New standards may create additional equipment testing requirements that the laboratories must be capable of performing.

The laboratory recognition process promotes the user community's confidence in, and acceptance of, test results from recognized laboratories. All equipment suppliers that participate in the P25 CAP must use recognized laboratories to conduct performance, conformance, and interoperability tests on their products. P25 equipment suppliers will release standardized Summary Test Reports (STRs) from recognized laboratories along with SDoCs. This documentation will be available on a publicly accessible Web site (<http://www.rkb.us>) to help equipment purchasers make informed decisions. The response community will be able to select from multiple vendors that build innovative products based on the same standards. Ultimately, this documentation will increase the public's confidence in the performance, conformance, and interoperability of P25 equipment.

With the first set of test laboratories recognized, P25 manufacturers will begin to submit their equipment for testing. A six-month grace period provides laboratories time to perform the tests outlined in the Baseline Common Air Interface Testing Requirements Compliance Assessment Bulletin. During this grace period, equipment delivered to agencies receiving Federal grant funding will not be required to have a supporting SDoC and STR; these grantees will be able to use the grace period to determine a date by which the manufacturer will provide the appropriate SDoCs and STRs. Grantees taking delivery of equipment after the six-month grace period has ended must confirm SDoCs and STRs exist for the relevant equipment purchased.

The P25 CAP will continue to accept applications from interested laboratories, further expanding the pool of laboratories from which manufacturers may test their equipment.

# Global Positioning System Technology Connects Emergency Responders with Resources

**G**lobal Positioning System (GPS) was originally developed with the purpose of finding our troops on the battlefield; today, it is responsible for helping millions of travelers locate themselves on the world's public roads. The technology has also begun to find its way into the cache of the emergency response community's most commonly used tools. When GPS is joined with wireless connectivity and geographic information system technologies, the result goes beyond navigation to track assets and people. This triumvirate of technologies enables real-time tracking, thereby creating situational awareness for key decision makers. Furthermore, when this information is shared among agencies, their staff can better communicate because they are working under a common operating picture.

One of the primary uses of GPS is in the Automatic Vehicle Location (AVL) technology. AVL has been adopted by ambulance, fire, and law enforcement agencies across the Nation. This capability enables dispatch services to locate resources closest to the emergency. When seconds count, the ability to quickly connect emergency responders with the resources they need can save lives. Newer AVL systems integrate an emergency vehicle's display computer, or data terminal, with records management and video systems. These data terminals can report the mechanical status of the vehicle's engine or other systems in real time. With this information, dispatch centers can track what resources are in use throughout their region.

Among its many benefits, AVL increases the efficiency of emergency response as a whole. AVL has improved dispatch services by providing data for planning police patrol areas, and it has been used to monitor police cars to determine if they are idle for long periods of time. Donald Ingrasselino, Elmwood Park (New Jersey) Police Chief, says, "Officers may think twice about sitting in their car for an hour with a cup of coffee."

If AVL increases efficiency, why don't more agencies use it? One reason is cost—it can cost thousands of dollars to equip a car not just with the GPS sensor, but with the wireless connectivity to transmit the vehicle's location back to the dispatch center.

Another reason for slow adoption may be privacy concerns. The debate is well summarized by a passage from the article "AVL— a Useful Tool or a Big Brother?" written by Penny Peters for the Michigan police newsletter, CLEMIS Times:

"Many officers believe that having AVL on their vehicles is just another way for the public or their bosses to keep an eye on their every move. That was not the case when Sterling Heights Police Department wanted to see where slain Officer Mark Sawyers had traveled the night he was stalked and gunned down by defendant Timothy Berner."

Offsetting concerns of privacy is AVL's aid to officer safety. The City of Oakland, California, has reported that retracing the route of a slain officer enabled police officers to retrieve the surveillance video leading to the capture of the killer. In Schaumburg, Illinois, AVL has been in use since 1992, and has played a role in at least two traffic stops that went awry. On one occasion, a police officer called for backup without describing his location, and on another, an officer pressed his emergency call button before being incapacitated. These are just two examples demonstrating AVL's GPS capability to promote officer safety. Across the Nation, AVL is acknowledged for its role in protecting officers in the field.

## OTHER USES OF GPS

### Resource Tracking

Emergency planners and responders may attach GPS-enabled "tags" to valuable resources such as generators, trailers, helicopters, and food. Known as Total Asset Visibility, many agencies are finding it invaluable to know—and see on a map—the exact location of everything they need to prepare for emergencies. Responders are able to monitor these locations in real time during large-scale events. When any tracked items are stolen, recovery is aided by knowing the exact location of pilfered property.

### Offender Tracking

GPS devices may be strapped to an offender's ankle to track their location. In addition to using GPS technology, newer models can operate indoors using cell-phone tower locations. Newer models can also disseminate alerts if boundaries are violated and even receive voice messages.

### Suspicious Vehicles

GPS tracking devices are updated versions of the homing devices that have been placed on vehicles for years. Where the old devices needed to be followed with a direction finder, the new versions create a moving dot on a map that is located at

information center headquarters, on smartphones, or in car-mounted data terminals. Using magnets, these devices are placed on vehicles where they cannot be seen. Currently, a model is now in development that can shoot a laser-guided air gun. This model will be mounted in the grill of a police car and will help lessen the number of dangerous high-speed chases.

### History At-a-Glance: How Does It Work?

GPS is based on a "constellation" of satellites, each of which broadcasts its precise location and the exact time of each signal. A GPS receiver looks at the time required for signals to arrive from three or more satellites, uses that duration to calculate its distance to each satellite, then uses triangulation to calculate the GPS receiver's location on Earth.

In recent years, cell phones have begun to incorporate GPS technology. Cell phones that use GPS create another approach to tracking people; that is, the geolocation of a phone can be tracked, and by extension, the person using that phone.

There are also devices—roughly the size of pagers—that are strictly GPS tracking devices. While these smaller devices are not cell phones, the geolocation of these devices are found through the use of cell phone chips and cell phone data access accounts. These devices can be slipped into a pocket, worn like a wristwatch, or attached to an object to enable the tracking of an object of interest, such as an officer or offender. For example, if an offender was located but not apprehended, an officer could attach the small GPS tracker to a material possession of the offender, such as their car.

### Organizing Information

The progress of accessible technology in smaller and cheaper forms with improved telecommunications has allowed GPS to advance from simple navigation abilities to more complex, real-time device tracking capabilities. At the same time, there has been a proliferation of mapping systems that aggregate information such as weather, shelter locations, water levels, and the location of those receivers, belonging to either officers or their vehicles. This aggregation creates the context of location and transforms a plethora of unorganized facts into actionable knowledge. The ability to locate resources in real time is a key advantage of a common operating picture.



When GPS is joined with wireless connectivity and Geographic Information Systems, the result goes beyond navigation to tracking assets and people...



IN YOUR OWN WORDS • • • • •

By Inspector Lance Valcour, Secondment to the Canadian Police Research Centre

## Interoperability Across Borders

As a 33-year veteran of the Ottawa (Canada) Police Service and the current lead for interoperability efforts on behalf of the Canadian Association of Chiefs of Police, Fire and Emergency Medical Services groups, I know that interoperability is a complex and multi-faceted challenge. Too many times to count, I have witnessed the pitfalls that arise from a limited ability to communicate with neighboring partners from different disciplines and jurisdictions. Encouraging emergency response agencies to consider the interoperability challenge from a cross-border perspective, incorporating international lessons learned, and improving science-and-technology-based research are just three ways Canadian and U.S. officials are working together to improve public safety.

Cross-border communications contribute to the interoperability challenge in a host of administrative, organizational, and operational ways. Our responders are required to move back and forth across international boundaries on a regular basis and need to be able to communicate effectively with each other.

Canada and the U.S. hold several of the world's busiest border crossings, as billions of dollars are traded across these borders every day. Responders from coast to coast—including the Alaska borders with British Columbia and the Yukon Territory—face unique challenges in managing their responsibilities along the longest common border in the world. While these officers are required to respect these “lines on a map,” criminals, fires, floods, and other natural disasters do not!

For example, we encounter situations that require paramedics to transfer hospital patients between Canada's Province of Ontario and New York State. On other occasions, fire fighters—often volunteers with limited communications budgets—need to provide mutual aid to their partners between the borders of Vermont and Quebec. In the spring of 2009, cross-border communications were tested once again when North Dakota experienced major floods that flowed into Canada's Province of Manitoba. The severity of this natural disaster combined with the number of affected citizens warranted the inclusion of support from neighboring agencies, including ours. Canadian and U.S. public safety officials worked closely together to manage this emergency, as they have for decades.

Even though these situations regularly require emergency responders to communicate, many units are not equipped to implement communications that can cut across disciplines and jurisdictions. Furthermore, emergency response groups are often unaware of the resources that are readily available to improve interoperable communications. This makes working collaboratively and gleaning lessons learned from other response units all the more important. If emergency response agencies around the globe regularly sought to incorporate lessons learned from other public safety groups, imagine the resultant positive impact. More effective standard operating procedures (SOPs) would exist, and communications as a whole would improve throughout both of our countries.

Gathering together to discuss best practices is not a new idea and can often be accomplished with little extra cost. Across the U.S. alone, meetings open to any members of the emergency response community are regularly held to discuss critical interoperability issues. The *National Emergency Communications Plan* (NECP)—a plan outlining recommendations and measurable goals for local, tribal, state, and Federal agencies to establish minimum levels of interoperability—is just one of the many governance policies that are in place to help U.S. states identify and act upon available emergency communications resources. Canada took note of this lesson learned in the U.S. and is currently developing the Canadian Communications Interoperability Plan (CCIP). Like the NECP, this Plan will focus on critical issues such as standard SOPs, joint cross-border exercises, and training. Our emergency response units and their governing bodies can see the benefits of both the CCIP and NECP. Both countries are working closely together via Public Safety Canada and DHS's Office of Emergency Communications and Command, Control and Interoperability Division to find concrete ways to improve the current state of cross-border interoperable communications.

Public safety communications are not a textbook problem; therefore, we cannot rely on textbook methods alone. Regularly sharing best practices and working together on science and technology projects will enable emergency response groups to leverage ideas from one another and implement more effective long-term solutions. This means that emergency response groups need to move across borders, familiarize themselves with the international responders with whom they are serving, and identify interoperability commonalities and challenges. Unless emergency responders approach the interoperability challenge from an international perspective and work toward common goals with real timelines, the cross-border interoperability challenge will have little chance of improving. And this can be done at little cost—sometimes for the price of a couple cups of coffee.



### Interoperability Infiltrates Georgia from Page 1

Before the Network is introduced into a region, the State holds workshop meetings with regional officials, GTRI representatives, and the vendor to discuss standard operating procedures (SOPs) and training opportunities. With only a handful of agencies still awaiting implementation, the State anticipates full network integration by 2010. The State is already looking to expand the GIN to encompass secondary public safety agencies such as the Department of Forestry and the Department of Transportation.

As the GIN continues to expand across the State, it will become more useful in large-scale incidents where multiple players are involved. Chief Information Officer of the Georgia Department of Public Safety and Chairman of the Homeland Security Public Safety Communications Task Force Dan Brown states, “The GIN is flexible and scalable, so a user can build single or multiple patches or call groups based on the size and scope of the event.” This capability is vital during larger scenarios in which radio systems are often overwhelmed by multiple voices. The GIN allows the Communications Unit Leader or on-site commander to decide who to connect to the main radio channels; this capability helps streamline communications, ensuring that the most urgent messages are heard. Brown notes, “If you're the operations leader for an event, you don't want everyone on the radio. Communications need to be segregated by the principles of the Incident Command System; it's the only way we can respond to these events and ensure that everyone has the radio time they need.” A series of SOPs have been developed and vetted with each participating region to establish guidelines for use of the GIN. These SOPs ensure the GIN is compliant with the Incident Command System and National Incident Management System.

In order for the GIN to reach its maximum effectiveness, each participating region must understand how to employ the Network. Before this can happen, additional SOPs will need to be created, instituted, and understood by participating regions. GEMA and GTRI have made training a priority throughout the implementation process to ensure that responders are well versed in the GIN before using it during a live event. According to McCook, “Working with the State, GTRI plans to implement tabletop and full-scale exercises for the system in the next 6-18 months.” These large-scale exercises will educate users on how to use the system during both major incidents and daily operations.

Looking to the future, the State plans to use the GIN to partner with neighboring states, including Florida, North Carolina, South Carolina, and Tennessee. Currently, the State is working to interconnect the GIN and the Florida Interoperability Network. As the Network grows, the State will be better prepared for major events and natural disasters, such as hurricanes. Ultimately, the GIN will improve collaboration and interoperability among the states, as it did within Georgia's emergency response community.

## Dereck Orr: Accelerating the Adoption of Critical Public Safety Standards



Since December 2002, Dereck Orr has served as the Program Manager for Public Safety Communication Standards at the National Institute of Standards and Technology's Office of Law Enforcement Standards. In this role, Orr leads a program that provides an objective technical advisor and laboratory to the U.S. Department of Homeland Security (DHS) and the emergency response community. Additionally, Orr leads a team that works tirelessly to accelerate the adoption and implementation of the most critical public safety communications standards and technologies.

Orr previously served as the Chief of Staff for the SAFECOM program within the DHS Science and Technology Directorate, where he helped to launch many new, groundbreaking programs such as the RapidCom initiative. Orr previously served as the Chief of Staff for the SAFECOM program within the DHS Science and Technology Directorate, where he helped launch many new, groundbreaking programs such as the RapidCom initiative. This initiative was launched to strengthen incident commanders' ability to adequately communicate with each other and their respective command centers within one hour of a major incident. Prior to his work

with SAFECOM, Orr was responsible for the appropriations accounts relating to state and local law enforcement issues as a professional staff member of the Senate Appropriations Subcommittee for the Departments of Commerce, Justice, and State, and related agencies under Senator Fritz Hollings.

### Q&A with Dereck Orr

**Q: From a scientific standpoint, what would you like to communicate to emergency responders about the interoperability challenge?**

A: From a technical perspective, one challenge we have faced has been the pursuit of continuous user involvement. While it can be easier to sustain public safety user participation for one week of testing, it is challenging to find entire groups that will stay involved continuously over the course of a five-year period. There are times when we even provide funding, but we still experience the challenge of enlisting long-term participants. At testing iterations, our teams represent the technical experts and can determine what technical next steps need to be taken, but we are not members of the emergency response community. We very much need their presence so their voice can be extended to manufacturers.

Project 25 (P25) meetings, for example, take place four times a year for one week at a time. One entire segment of the meeting addresses user requirements. We need as many emergency responders as possible to participate in that segment to keep us better informed of the regular problems they encounter. It can be difficult to track a problem's progress if responders are not continually sharing that progress. It is important to have a multi-geographic, multi-discipline point of view. When only one voice is participating in these meetings, then standards suffer.

**Q: What foreseeable solutions are on the horizon to address the challenge of user participation?**

A: In order to maintain user involvement for a long period of time, we are regularly looking for effective ways to communicate what milestones have occurred in these technology arenas. Through additional communication

with the emergency response community, we hope responders will better leverage these advancements. It seems like every conference or special public safety event I attend, I find another group of people who are not aware of the relevance of standards, which raises the question: how can we get this information out uniformly on a national basis?

While actively engaging the practitioner community is a sizeable challenge, we do not consider it a pipe dream. We are looking to leverage new technologies and processes like WebEx seminars. These types of remote communication methods allow attendees to easily participate, regardless of their location.

**Q: From your position, what are easy steps that emergency response groups can take to improve interoperability throughout their unit?**

A: My primary answer here would be that emergency response groups can prioritize the use of standards to leverage the capabilities of their unit. Units improve their interoperability by implementing available standards. By using equipment that is developed to meet certain specifications and standards regardless of the manufacturer, agencies alleviate a major challenge on the path toward complete interoperability.

**Q: What technologies and initiatives are you most excited about?**

A: Since the first set of laboratories has been approved to test P25 radio equipment, my team is looking forward to seeing the P25 Compliance Assessment Program become more widely accessible to the emergency response community. This Program will ensure that public safety officials can have a higher level of confidence in the equipment they are purchasing.

We are also looking forward to the continued development of Voice over Internet Protocol (VoIP) standards for new VoIP products, as well as scientifically identifying audio quality issues that public safety officials experience with their digital radios.

With Radio over Wireless Broadband technology, we continue to discover new ways to link existing land mobile radios (LMRs) with broadband data networks and multi-band radios. Our teams are always looking toward new technologies that will allow the emergency response community to achieve interoperability with greater ease than ever before.

**Q: In the next 5 to 10 years, what interoperability advancements would you like to see across the emergency response community?**

A: I would love to see the widespread application of core standards. The implementation of these standards would allow a minimum level of voice communications across LMR, digital broadband systems, and the commercial cellular network. As I mentioned before, this cannot be achieved without the consistent help and input from emergency responders about the technologies they use. P25 is just one example of an initiative that could not have made such significant progress without participation from practitioners.

To participate on a long-term basis in the testing of core standards, please contact Dereck Orr at [Dereck.Orr@nist.gov](mailto:Dereck.Orr@nist.gov).

# States Work Together to Implement an Open Information Sharing Network

In the wake of Hurricanes Katrina and Rita, the devastated regions realized they must establish more effective and open lines for information sharing across state lines. Many states and communities are in the process of purchasing and deploying their own unique visualization and resource analysis tools that will support the decision making of state homeland security and emergency management officials. The southern states are employing a locally-driven, system of systems approach built upon standards-based, open architectures to tackle the issue of interstate information sharing. Using this approach, these states are developing an integrated set of processes and solutions that complements existing policies, processes, and architectures in each of the respective states. The Regional Operations Platform Pilot (ROPP) aims to achieve seamless information exchange among participants, as needed and as authorized. The ROPP is supported by the Command, Control and Interoperability Division within the U.S. Department of Homeland Security (DHS) and the DHS Science and Technology Directorate's First Responder Technologies program. Working together through this Pilot, participating states will develop a national model that enables information sharing across stakeholder organizations. This model will ultimately improve incident management and day-to-day response efforts.

During a two-day session in Mobile, Alabama, in February of 2009, state homeland security and emergency management representatives from Alabama, Florida, Georgia, Louisiana, Mississippi, Tennessee, Texas, and Virginia met to kick off the ROPP. During the meeting, representatives discussed proactive information sharing initiatives, current elements that may impede their ability to share information within and across state lines, and possible solutions to overcome these obstacles. Discussion topics included the need for standard operating procedures and a governance framework, bandwidth and connectivity issues, the exchange of proprietary information, access control, maintenance of a bottom-up approach, Federal offerings, local buy-in, and a standard symbology.

Participating states agreed that increased information sharing will improve decision making and situational awareness during daily operations and large-scale emergency response initiatives. With DHS support, participating states are currently working to define user requirements for a solution that addresses these issues. Once agreed upon, these requirements will be validated through a capstone exercise and replicated in other jurisdictions across the Nation.

Since the kick-off meeting, ROPP participants have formed operations and technical working groups that meet on a bi-monthly basis. Each working group has designated a liaison who communicates the group's discussion outcomes and progress so that all participants are closely linked into all project developments. Currently, the technical working group is identifying a full inventory of available data layers, which will inform follow-on user requirements sessions. Concurrently, the operations working group is in the preliminary stages of planning the capstone exercise that is scheduled to be executed in the fall of 2009. During this exercise, states will validate a series of technical integration efforts and operational best practices that will serve as a national model for seamless multi-discipline, multi-jurisdiction information sharing. This real-time exercise will make tremendous strides on the path toward improving regional preparation, protection, recovery, and response efforts among the partner states. A comprehensive resource guide of best practices and lessons learned will be available to all interested jurisdictions following completion of the exercise. The ROPP resource guide will also be used as a baseline to the broader follow-on DHS effort: Virtual USA.

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

PRESORTED STANDARD  
U.S. POSTAGE PAID  
SUBURBAN, MD  
PERMIT NO. 4889

## Interoperability TECHNOLOGY Today



Homeland  
Security

A Resource For the Emergency Response Community

- Summer edition 2009  
"This edition features..."
- Interoperability Infiltrates Georgia's Emergency Response Agencies
  - Information Sharing and Virtual USA
  - Laboratories Approved to Test Project 25 Radio Equipment
  - Global Positioning System Technology Connects Emergency Responders with Resources
  - Interoperability Across Borders
  - Spotlight on Dereck Orr
  - States Work Together to Implement an Open Information Sharing Network