Interoperability Technology Today

Homeland Security

A Resource For the Emergency Response Community

Spring 2007

High-Speed Pursuit of Interoperability

The bright lights of the Las Vegas Strip in Clark County, Nevada, annually attract tens of millions of visitors—some of them felons. High-speed vehicle pursuits may travel across multiple jurisdictions and involve more than a dozen law enforcement agencies. To successfully respond to these emergencies, police officers need to exchange vital communications. But agencies with incompatible radio systems, or ones that operate in different frequency bands, may not be able to communicate with each other. Standard operating procedures (SOPs) may vary from agency to agency—compromising a coordinated response as well as the safety of officers in the field. Interoperability can mean the difference between life and death.

"Policing is very mobile," says Dennis Cobb, Deputy Chief of Communications and Technology Services Division, Las Vegas Metropolitan Police Department (LVMPD). "One of the most common uses of radios across jurisdictions is in vehicle pursuits. There's a fast evolution and it's dynamic and unpredictable. Voice is a 'must have' compared to data, which is a 'nice to have.' Police use radio intensively and to position resources in front of and across greater distances. And it happens fast," he says.

While some of law enforcement's interoperability needs may differ from those of firefighters and emergency medical services (EMS), Cobb and others agree that achieving interoperability for law enforcement agencies is based on the same basic requirements all agencies face—regardless of emergency response disciplines.

More than Technology

The Office for Interoperability and Compatibility's (OIC) Interoperability Continuum graphically depicts five factors critical to a successful interoperability solution: governance, (SOPs), technology, training and exercises, and usage.

"Governance is by far the most critical [factor] in the interoperability ball game," says Tom Chirhart, OIC Spectrum and Interoperability Technologies Program Manager. "It's a ball game because it takes a team effort to win. If everyone can establish an effective interoperability committee, they've made it to first base. Second base merges SOPs and technology, because you can't develop a fully functional SOP without knowing the capabilities and limitations of the existing or legacy systems or technologies to be used." Chirhart knows both the operational side and the policy side of law enforcement. Previously a police officer and sheriff's deputy, he has also been a 9-1-1 center director and worked in radio for the U.S. Navy and the Coast Guard.

"Third base merges training and exercises with usage. Routine usage reduces the need for training," Chirhart says. "If you use the equipment or frequencies, there is no need to stop and dig out a training manual. Exercises expose the user to non-routine events and identify potential shortfalls in all five areas."

Cobb agrees that routine use of interoperability channels is imperative. Cobb manages a 9-1-1 center, which answers calls for fire response and EMS as well as police, and covers 8,000-square-mile Clark County and Las Vegas. "We're trying to make high-frequency, low-intensity use of the interoperable channels a commonplace event for all emergency services," says Cobb. "We're working on a procedure that would require checking in via the interoperability channels as part of the basic vehicle checkout. As they start their shifts, fire would call my dispatch center for a radio check, and when my sergeants go to their police cars, they'd call the fire alarm office over the interoperability channels. Just to remind them it's [the units] there."

Leverage Existing Systems

Cobb was appointed by the Governor to Nevada's State Interoperable Executive Committee (SIEC), and helped develop the original strategic plan for the state. "We had a bushel basket full of needs that weren't mapped very well to existing capabilities," says Cobb. "Our initial statewide assessment was to see what we actually had at that time." The SIEC decided to connect the mutual aid channels by bridging four large networks in Nevada, making the core systems responsible for tying in their smaller mutual aid partners. As these four networks are bridged, the state may use a legacy 150 MHz system as an interoperable backbone for rural agencies in Nevada, tying the backbone via the interoperable frequencies to the four core systems.

Four Corners Regional Collaborative

The Regional Four Corners Homeland Security Coalition (R4C), named for where the boundaries of Colorado, Utah, New Mexico, and Arizona abut, is also taking a regional approach in a project that involves all tribes and all counties located within the states. Setting up a strong governance process is

continued on page 6

Disaster Management Wins Excellence.Gov Award

On February 20, the Industry Advisory Council's Collaboration and Transformation Shared Interest Group announced the Disaster Management (DM) program as one of five program winners for the seventh annual Excellence.Gov awards. The theme for this year's awards was Information Sharing. Award winners have demonstrated excellence in leveraging technology to enhance collaboration. Winners presented their lessons learned and best practices in Washington, DC.

The DM program received an Excellence. Gov award for its critical work in developing interoperable and collaborative information sharing tools for the emergency response community. DM enhances information sharing by: facilitating practitioner-driven incident management data standards, providing a free incident management toolset, and supplying an information and collaboration Web portal. The Excellence.Gov award is a testament to DM's valuable contributions to the emergency response community as well as to citizens nationwide.

CONTENTS

About Interoperability Technology Today

The Department of Homeland Security (DHS) established the Office for Interoperability and Compatibility (OIC) in 2004 to strengthen and integrate interoperability and compatibility efforts in order to improve local, tribal, state, and Federal emergency response and preparedness. Managed by the Science and Technology Directorate, OIC is assisting in the coordination of interoperability efforts across DHS. OIC programs and initiatives address critical interoperability and compatibility issues. Priority areas include communications, equipment, and training.

OIC is creating the capacity for increased levels of interoperability by developing tools, best practices, and methodologies that emergency response agencies can put into effect immediately, based on feedback from emergency response practitioners. OIC is also improving incident response and recovery by developing tools and messaging standards that help emergency responders manage incidents and exchange information in real time.

Interoperability Technology Today is published quarterly by OIC 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.

Subscriptions: *Interoperability Technology Today* is available at no cost. If you are not currently on our mailing list, please call toll free 866-969-SAFE (7233), or visit the SAFECOM program's Web site, 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. Call toll free 866-969-SAFE (7233), or visit www.safecomprogram.gov, the SAFECOM program's Web site, 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 spring 2007 edition of *Interoperability Technology Today*, published by the Department of Homeland Security, Office for Interoperability and Compatibility, 866-969-SAFE (7233)," should be included.

Photo Credits: Photos and graphics used in this edition of *Interoperability Technology Today* include Thinkstock® & Getty®.

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

Homeland Security

Upcoming Events

Events & Conferences

OIC Industry Roundtable
May 9-10, 2007
Washington, DC
http://oic.csrincorporated.com/

Association of Public-Safety Communications Officials International 73rd Annual Conference & Exposition
August 5-9, 2007
Baltimore, Maryland
http://www.apco2007.org/

International Association of Fire Chiefs Fire-Rescue International
August 23-25, 2007
Atlanta, Georgia
http://www.iafc.org/displaycommon.cfm?an=1&subarticlenbr=356

DIRECTOR'S MESSAGE

By Dr. David Boyd

Emergency responders are steps closer to having the capacity to seamlessly exchange critical data— situational reports, requests for personnel, maps, availability of hospital beds—across disparate software systems and applications.

Last year, the Office for Interoperability and Compatibility's (OIC) Disaster Management (DM) program worked with practitioners to develop and submit three standards—the Distribution Element (DE), Resource Messaging (RM), and Hospital AVailability Exchange (HAVE) Standards—to the Organization for the Advancement of Structured Information Standards (OASIS):

- The DE standard provides a flexible message distribution framework for the sharing of data by emergency information systems. This standard enables responders to distribute data messages by recipient, geographic area, or other specifications such as discipline type.
- The RM standard will enable responders to exchange resource data—including personnel and equipment needed to effectively support emergency preparedness, response, and recovery.
- The HAVE standard will enable responders to exchange information about a hospital's capacity and bed availability with medical and health organizations.

OASIS adopted the DE standard in April 2006, and is expected to adopt the HAVE and RM standards this year.

DM also supports the Common Alerting Protocol (CAP), a standard that enables practitioners to exchange all-hazard emergency alerts, notifications, and public warnings. Such data can be disseminated simultaneously over many different warning systems, e.g., computers, wireless, alarms, television, and radio. OASIS adopted CAP in October 2005.

Incorporating these new data messaging standards into information sharing products will strengthen recovery and response during day-to-day operations and large-scale emergencies.

A practitioner-driven approach was and is essential to ensuring these standards effectively meet the needs of responders in the field. Throughout the standards development process, DM works closely with its Standards Working Group, comprised of practitioners, industry leaders, and representatives from other Federal information sharing efforts. DM also collaborates with private industry, encouraging a speedy implementation of practitioner-driven standards into software, systems, and devices. By including industry, DM's standards development process also generates more products that meet practitioner requirements.

The development of these standards represents significant progress, but much work remains. DM is working with emergency responders to develop a Situational Awareness Messaging Standard (SitReps). SitReps will provide practitioners with data about an emergency's situation, including what resources are needed prior to, during, and in recovery from, an emergency.

Partnerships will continue to be key as DM advances the development of standards for information sharing. DM participates in the National Information Exchange Model (NIEM), a partnership between the Departments of Justice and Homeland Security. NIEM allows local, tribal, state, and Federal governments to effectively share critical information in emergencies, and supports the daily operations of agencies nationwide. DM also works with the Emergency Interoperability Consortium (EIC), an industry group that works to promote the design, development, release, and use of Extensible Markup Language standards to help solve data-sharing challenges encountered during emergency response.

"The DM and EIC collaboration demonstrates how effective public/private partnerships can be in addressing core issues that impact commerce and technology," says EIC Chair, Matt Walton. "The global adoption of CAP, and the expanding proliferation of the DE and HAVE, provide a solid foundation on which to build an open framework that will ultimately benefit government, industry, and those in need."

A fundamental success of the DM standards initiative is this type of collaborative effort—multiple entities working together to conceive, develop, adopt, and execute standards that responders can use everyday to protect the lives of those in the field as well as victims awaiting help.

Gateways: Bridging Gaps for the Near-Term

During a coordinated emergency response, agencies from different jurisdictions—even those with sophisticated radio systems—may have to rely on runners or multiple dispatchers to relay messages among responding agencies. The reason—emergency response agencies with incompatible radio systems, or ones that operate in different frequency bands, often cannot communicate with each other.

For many agencies, gateways have offered a near-term solution to bridging these gaps. Gateways provide connections between two or more disparate radio networks, allowing users on one network to communicate with users on other networks.

The three principal types of gateways are:

- Portable gateways are used on a temporary basis to link two or more radios to create two or more separate radio talk paths. Portable gateways can be carried in a vehicle and quickly deployed by attaching portable radios to one on the scene, mostly for line-of-sight communications.
- Mobile gateways are typically installed in a command or communications vehicle; mobile radios and fixed antennas are placed on the vehicle's roof. Typically used to enable temporary communications, these gateways can achieve line-of-sight or repeated interoperable communications.
- Fixed gateways are the most robust of all gateway configurations. Fixed gateways can be used on either temporarily or permanently. They are generally installed in or near an emergency communications center. Some fixed gateway systems are incorporating Voice over Internet Protocol, allowing systems to support larger geographic areas.

Some gateways also connect to cellular or public switched telephone networks.

Although varied in architecture, all gateway configurations are based on a common principle: a system receives a radio transmission on one frequency and patches audio to one or more other agencies using the frequencies of the other agencies' radio channels.

This technology was potentially life-saving for agencies responding to the 2002 sniper attacks in the National Capital Region (NCR).

"During the sniper incident in 2002, lots of agencies from different jurisdictions [in the NCR] converged on the crime scenes. We were not prepared to handle communications for a coordinated response of this magnitude. A mobile gateway system enabled communications among the agencies," says Captain Eddie Reyes of the Alexandria, Virginia Police Department.

Because they can be installed without significant radio infrastructure modifications, gateways are a popular technology solution for localities that have not received sufficient funding to standardize radios. Further, gateways are capable of interconnecting multiple HF, VHF low band, VHF high band, UHF, 700 MHz, 800 MHz, and 900 MHz radios—offering considerable functionality. Despite these advantages, Reyes notes that gateways should be used only as an interim interoperability solution as an agency moves toward a shared, standards-based system.

To some, gateways yield more costs than they do benefits. Gateways are inefficient: they require twice as much spectrum, because each participating agency must use at least one channel in each band per common talk path. Typically, a gateway's operation can be limited to the geographic coverage area common to all participating systems. Uncoordinated use of gateways has also been known to wreak havoc on radio systems—disrupting critical communications.

Because most gateways are controlled by an operator-directed computer system, faulty communications are typically the result of human error. "A poorly engineered gateway at the hands of a person with no training can be a real disaster to public safety communications," says Reyes.

Charles Werner, Fire Chief of the Charlottesville, Virginia Fire Department, says that planning, policies, procedures, and training are a must for a gateway to be of value to agencies coordinating a response.

"One of the lessons learned from the Hurricanes in Florida was that they had responders in the field and many devices to connect responders, but they didn't always have the technical personnel required to support all of the gateways," says Werner.

Werner also notes, "There is one main variation between gateways—those that are simple 'plug and play' (don't require programming) and those that require programming. In the settings [that] are routine and anticipated, the programmed gateways can be preprogrammed. It's when new [unexpected] agencies must be added—that requires the special programming in the field."

The three "R's" for successful gateway operation:

- Readiness training: An agency can designate a number of responders to receive formal manufacturer training. Nobody knows the equipment better than the manufacturer. With time, those trained on the device can train other responders in the agency.
- Routine use and testing with multiple agencies: Regular training with all regional agencies that would use the system in an emergency helps ensure that all network components function properly.
- Regular maintenance: It is important to make sure a gateway's radio programming is up-to-date—reflecting any changes in an agency's frequency or talk group.

Tips for Agencies Considering Gateways:

- Determine how the gateway will be used, e.g., tactically or as a fixed system.
- Determine what type of technical support the gateway will require.
- Determine the reasonable number of agencies that will use the gateway system.
- Consider whether the gateway meets durability standards to survive the wear and tear of field operations.
- Consider operational cost implications for maintenance and sustainability.
- Plan for adequate technical and operational training.

Benchmarking Success with Standards Working Group

By Timothy Wiedrich, Section Chief, Emergency Preparedness and Response, North Dakota Department of Health

In June 2005, the Disaster Management (DM) program made significant strides when it brought key emergency management stakeholders to the table. This assembly marked the first meeting of the Emergency Data Messaging Standards Working Group (SWG).

We represent diverse perspectives—those of emergency response agencies, industry, technical specialists, and standards development experts. But we share a common goal: to develop data messaging standards that meet the needs of practitioners in the field, and to help industry incorporate these standards into technology solutions. By bringing together key stakeholders, the SWG leverages the valuable input and first-hand experiences of members—ensuring that the development of data messaging standards is driven by practitioner requirements, and meets industry needs.

Data messaging standards are critical to our ability to save lives. Disparate software systems often prevent the exchange of vital emergency information—compromising preparedness, response, and recovery

continued on page 5

Innovation and Cooperation in the Lone Star State

Texas Council of Governments: Regional Partnerships

The Dallas region's locally driven approach and commitment to partnerships have proven invaluable to overcoming the challenges of implementing a regional communications framework. Since September 2002, Texas has leveraged 24 Councils of Government regions to ensure that homeland security planning and execution occurs on a regional basis, with local officials working together closely across all jurisdictions and disciplines. During the Dallas Love Field Wireless Integration Project, the North Central Texas Council of Governments (NCTCOG) was actively involved to ensure that new emergency responder communications supported regional interoperability goals. The NCTCOG serves a 16-county region of North Central Texas, which is centered around the two urban centers of Dallas and Fort Worth. NCTCOG was established to assist local governments in planning for common needs, cooperating for mutual benefit, and coordinating for sound regional development. NCTCOG's purpose is to strengthen both the individual and collective power of local governments and to help them recognize regional opportunities, eliminate unnecessary duplication, and make joint decisions.

The City of Dallas, Texas, has achieved interoperable communications for the region's emergency responders—all for less than the cost of a new squad car. This milestone represents a significant step toward implementing a statewide interoperable communications system.

Through regional cooperation and an innovative, service-based approach, Dallas successfully established a communications framework that uses existing equipment and spectrum. The new system provides aviation officials, industry partners, and the region's emergency responders—including more than 5,000 law enforcement officers, firefighters, and emergency medical service responders—with the capacity to exchange voice, video, and data across diverse networks.

"It is important that I have the ability to communicate not only with my firefighters but also with other agencies—we are the first line of defense when it comes to man-made and natural disasters," said Dallas Fire Chief Eddie Burns, Sr. at the Dallas Love Field (DLF) press conference, held September 14, 2006. "Having the ability to talk with other cities, other departments, and other agencies will enhance the capabilities of all first responders."

Interoperability progress in Dallas gained momentum in May 2005 through the partnering of the State of Texas, the City of Dallas, the Texas congressional delegation, the North Central Texas Council of Governments (NCTCOG), the U.S. Department of Homeland Security (DHS), and a Seattle-based technology company in order to implement a communications framework at DLF. Initiated in collaboration with the State of Texas Governor's Office of Homeland Security, the DLF Wireless Integration Project was funded by a $979,100 grant from the DHS Information Technology and Evaluation Program, which is co-administered by the Department's Office of Grants and Training and Office of the Chief Information Officer.

The project was designed with the goal of implementing a communications framework for a national interoperability service model that could be cost-effectively duplicated throughout Texas and the Nation. As Dallas is the first city in the Nation to use this national interoperable communications service, DLF project leaders see their city as a working model for regions nationwide.

DLF airport was chosen for the project because of the site's critical infrastructure, location in a major urban metropolitan area, and high concentration of diverse responder agencies and private-sector organizations.

"After this system was implemented at DLF, all participating local, state, and Federal agencies were interoperable—using their existing equipment for communications, and capable of sharing digital data and live video originating from the airport," says Terry Mitchell, Assistant Director of Aviation Operations for the City of Dallas.

Mitchell added that the communications framework also has strengthened information sharing and coordination among participating agencies and partners.

These participating agencies include:

- Dallas Fire Department
- Dallas Police Department
- Dallas Aviation Department
- Southwest Airlines
- Texas Department of Public Safety
- Texas Department of State Health Services
- U.S. Customs and Border Protection
- U.S. Centers for Disease Control
- U.S. Department of Health and Human Services
- U.S. Transportation Security Administration

The DLF project supports the interoperability goals of Texas leaders, who have long understood the gravity of ineffective communications. In keeping with their commitment to achieving interoperability, in 2004 the state released its Texas Homeland Security Strategic Plan, which included a roadmap for ensuring interoperable emergency communications. With the implementation of the DLF communications framework, the state made great strides toward establishing a statewide network of interoperable radio systems.

The DLF project also addresses communications breakdowns that compromised local response operations during recent large-scale disasters—including Hurricanes Katrina and Rita, and last year's Panhandle wildfires.

Service-Based Approach

Project participants began developing the interoperability service network in fall 2005. The project used an innovative technology developed and implemented by the Seattle technology company. This overlay software encryption technology is referred to as a Cryptographic Overlay Mesh Protocol. It creates a "network of networks" that enables emergency responders operating on different frequencies to seamlessly and securely exchange communications. The technology passed all qualification tests for certification under the Department of Defense's (DoD) Interoperability Communications Exercise 2006, certifying adherence to DoD interoperability standards.

In addition to enabling voice and data exchange, the software protocol provides Dallas agencies with real-time access to live video from existing cameras installed in airports, government buildings, police cruisers, and fire trucks. Network access and voice and data transmissions are secured by the Advanced

Lessons Learned from the Dallas Love Field Wireless Integration Project

- Consider a software-enabled service approach.
- Develop a plan and standard operating procedures to govern how, when, where, why, and who uses an interoperability system.
- Emphasize a regional, stakeholder-driven approach.
- Encourage innovative thinking and cooperation.
- Leverage existing infrastructure and resources.
- Practice frequent training on and use of an interoperability system; this is a must for a viable system.

Encryption Standard 256 (AES-256). AES-256 provides responders in Dallas with confidence they can securely exchange incident-related information without disruptions that could compromise the safety of responders in the field and those awaiting help.

"The Dallas Love Field Wireless Integration Project demonstrated the efficacy of integration technology in achieving radio interoperability," says Steve McCraw, Texas Homeland Security Director.

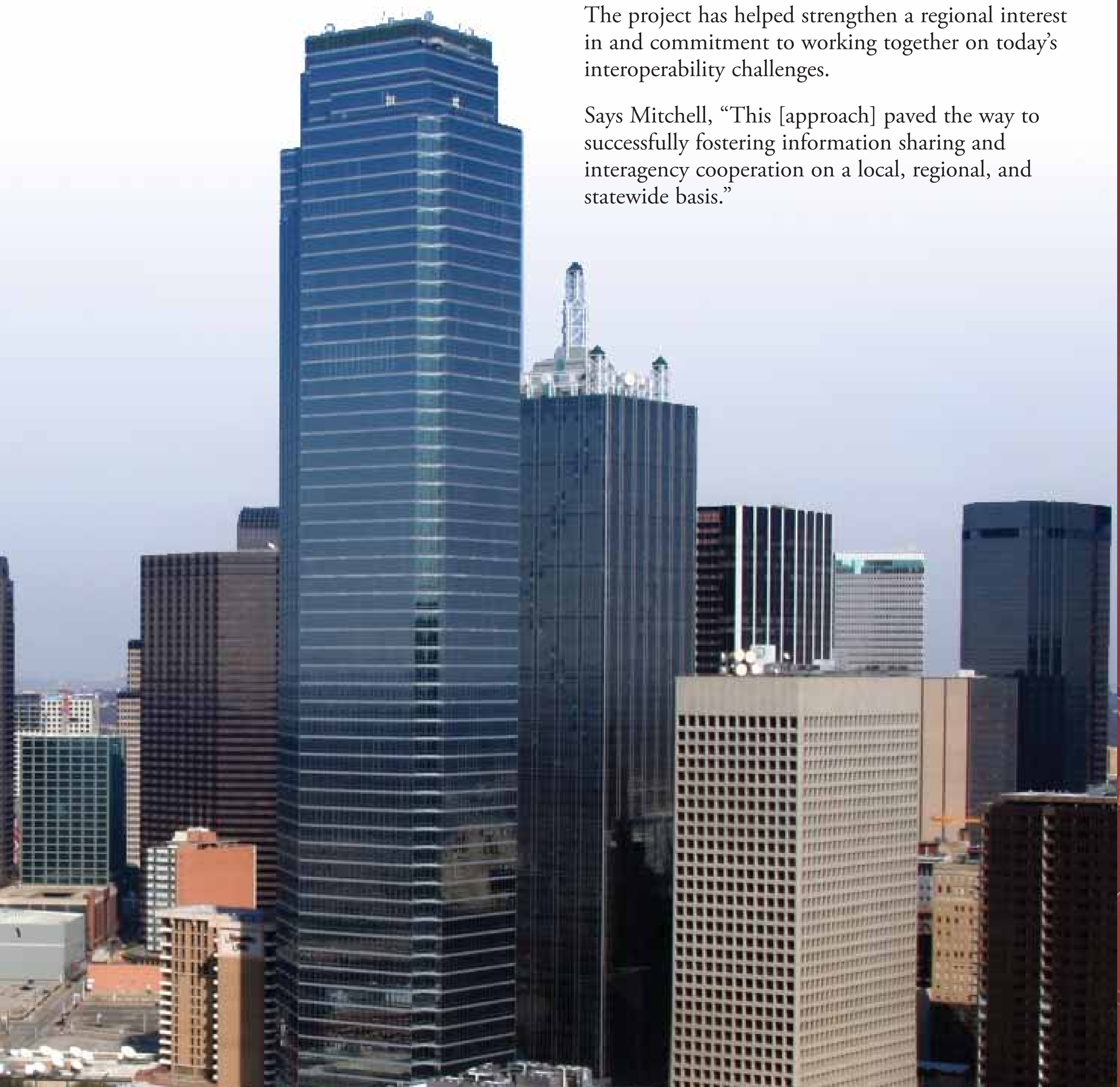
By creating a common interface that all available resources can share, the network of networks made the two-way radios of the Dallas agencies compatible with other radios and commonly deployed devices, including cellular phones, laptops, and personal digital assistants. Agencies using the service are able to control their levels of interoperability, and at all times know with whom they are exchanging information.

Leveraging Existing Resources

Like many emergency response agencies nationwide, agencies in Texas typically purchase communications equipment independently of each other. Many of these legacy systems work well only with equipment made by the same manufacturer. Even agencies with the newest equipment find that their radios cannot work with equipment from other manufacturers.

The software technology used for the DLF project addresses this challenge by providing interoperability across multiple, disparate networks. Rather than relying on the costly acquisition of new equipment, the framework leverages existing radio systems. Legacy devices are bridged onto the network through gateways enabled with overlay software. Use of existing resources has not only proven cost-effective for Dallas agencies, but also has reduced the implementation and training time for making the service operational.

The software also has allowed Dallas agencies to efficiently use fixed network resources, such as spectrum. Instead of loading networks with devices that deplete the operating capacity of the networks, the software creates a "mesh" architecture in which every device that accesses the network adds to the network, with each device acting as its own router, extending network reach.



Making Strides

These technologies have had a significant impact on the Dallas region's emergency response communications.

"In addition to interoperable radio communications, the system has provided us with the ability to share digital data and live video from Love Field among system users, which was previously unavailable," says Mitchell. "Voice communications between local, state, and Federal responders is now much easier to accomplish, and we no longer must share radios between groups."

"This is a must-have service. We must have interoperability among our radio communications," said Dallas First Assistant Chief of Police David O. Brown at the DLF press conference. "This is a potentially life-saving technology."

The subscription costs each local, state, and Federal agency or critical infrastructure partner $20,000 per year, which provides all of its responders and key personnel access to the interoperability service network. The service is offered on a nationwide basis.

Commitment to Partnerships

The DLF project's stakeholder-driven, cooperative approach has proven invaluable to this progress. Recognizing that disasters know no boundaries, emergency response leaders, local government officials, and private sector representatives—many with competing constituencies and communications requirements—joined to lead the DLF project.

The NCTCOG, which represents 16 counties in the Dallas-Fort Worth Metropolitan Area, coordinated the effort. The NCTCOG ensured that implementation supported: State of Texas interoperability plans, the Dallas-Fort Worth-Arlington Urban Area Security Initiative Tactical Interoperable Communications Plan, and the National Strategy for Homeland Security.

"Regional cooperation and partnerships played an important role and contributed to the project's overall success," says Mitchell. "A broad range of local, regional, and statewide partnerships provided valuable stakeholder feedback during the design and implementation of the project, ensuring that all stakeholder participant requirements were met."

The project has helped strengthen a regional interest in and commitment to working together on today's interoperability challenges.

Says Mitchell, "This [approach] paved the way to successfully fostering information sharing and interagency cooperation on a local, regional, and statewide basis."

Benchmarking • continued from page 3

efforts. Further, as information technology improves, software products may become more proprietary, multiplying the disconnect between the disparate systems.

Since the SWG's creation, we've achieved remarkable progress. One SWG standard has been adopted by the Organization for the Advancement of Structured Information Standards (OASIS), and two standards sets are currently under OASIS review that are likely to result in approximately 20 individual message standards. And we have work on the horizon.

The SWG is working with DM to develop a situational awareness messaging standard (SitReps). SitReps provides practitioners with data about an emergency's current situation, including what resources are needed.

Many times, the development of more than one standard is underway. So it will continue to be important for SWG members, industry, and the emergency response community to recruit subject matter experts so that resources meet development needs.

SWG members work closely with the DM program's Practitioner Steering Group (PSG), a practitioner-comprised body that provides input and recommendations regarding programmatic direction. SWG addresses the priorities and emergency response requirements identified by the PSG and collaborates with the PSG on draft standards.

The work of these groups, coupled with partnership efforts across government, industry, and the practitioner community, are essential to progress. Together, we are laying the groundwork for achieving data interoperability for our fellow responders on the frontlines.

Office of Emergency Communications Update

The Department of Homeland Security Appropriations Act 2007 (Public Law 109-295) establishes the Office of Emergency Communications (OEC). The Act transfers SAFECOM from the Office for Interoperability and Compatibility (OIC) to OEC. SAFECOM's authorities related to research, development, testing, evaluation, and standards will remain in OIC. The Act also transfers the Integrated Wireless Network and the Interoperable Communications Technical Assistance Program to OEC. OIC and OEC leadership are working closely together through the transition to ensure that SAFECOM's current activities remain on schedule. Once the transition is complete, OIC and OEC will continue to coordinate to successfully achieve SAFECOM's critical mission. Additional updates will be made in ***Interoperability Technology Today*** as the transition continues.

High Speed • continued from page 1

critical in a collaborative project like this, says Gary Edwards, Chief Executive Officer, National Native American Law Enforcement Association. "Everyone has an equal voice at the table," says Edwards. "As Secretary Chertoff recently noted, threats are risk-based and the consequences of threats are region-based, and DHS [Department of Homeland Security] has begun to look at regionalization as an important positive element in determining where money goes."

Initially, the R4C Coalition is addressing interoperable communications, information and intelligence sharing, and the protection of critical infrastructure and key resources regionally through an all-hazard, multi-discipline, cross-jurisdictional approach. "The focus is on utilizing the state, tribal, and county resources currently owned in the best way possible," Edwards says. "A capabilities baseline was designed to correlate current resources owned to capabilities, and next to compare regional capabilities possessed to the National Preparedness Goals for the region, based on a vulnerabilities/risk analysis.

"Capability gaps," Edwards adds, "will be identified between the 'As Is' capabilities and the 'Desired to Be' capabilities for the region. We believe the best way to compete nationally for additional homeland security funding, needed to make the region's citizens, critical infrastructure, key resources, and economy safe, is through collaborative regionalization."

Cultural and Operational Issues Key

"Since September 11, 2001, critical infrastructure protection has become a focus, and this has only magnified the mission significantly for agencies already strapped for funding," Chirhart says. "Many agencies have found major holes in their ability to communicate with surrounding agencies." Technology is not the key issue to resolving interoperability problems. In fact, Chirhart rates technology as a minor issue because many technological solutions are available today.

"We need to emphasize sharing before shopping," agrees Cobb. "If you're not sharing, why should I believe that buying new equipment will make you want to share? If you don't solve some of the cultural and operational issues first, you buy the wrong equipment," he adds. "But agencies don't have vendors knocking on their doors saying we'll help you change your culture and your operations. They're selling you their answer—an answer in a can— rather than recommending more difficult changes [that] in practice you can't buy."

Interoperable Communications Technical Assistance Program at a Glance

Emergency response agencies working to improve the procurement, implementation, and maintenance of their interoperable communication systems may find much needed help from the Interoperable Communications Technical Assistance Program (ICTAP). Managed by the Department of Homeland Security's Office of Grants and Training, ICTAP provides free, on-site technical assistance to local, state, and Federal emergency responders and officials in Urban Area Security Initiative (UASI) sites.

Through its assistance services, ICTAP is working to improve the capacity of emergency responders to communicate with each other on-demand. In keeping with this mission, the program helps UASI sites leverage existing resources, and provides services intended to strengthen interoperability planning, policy decisions, needs analysis, and implementation.

Last year, ICTAP provided UASI sites with assistance in developing their Tactical Interoperable Communication Plans (TICPs). ICTAP partnered with the Department of Justice's Office of Community Oriented Policing Services, or COPS, to provide regional training workshops on TICP guidance.

ICTAP has developed the Communication Assets Survey Mapping (CASM) tool software to help emergency response agencies capture radio communication infrastructure information. CASM provides regions with a snapshot of current interoperability capacities through a graphical mapping function. UASI sites will be able to leverage this tool to perform equipment inventories for their TICPs. SAFECOM is partnering with ICTAP to implement CASM, in order to support the goals of its Public Safety Architecture Framework (PSAF) effort. The PSAF tool will help emergency response agencies compare existing communications systems, and identify system gaps and points of interoperability.

Additional information about ICTAP is available at:
http://www.ojp.usdoj.gov/odp/ta_ictap.htm

SPOTLIGHT

Blazing the Trail in Virginia

As a volunteer firefighter for 26 years, Jim Junkins is well-versed in the necessities and challenges of interoperable communications. Today, Junkins serves as Director of the Harrisonburg-Rockingham Emergency Communications Center (HRECC) in Harrisonburg, Virginia.

As project manager of the county's regional radio system, Junkins is leading an effort to implement a communications system that will link 31 emergency response agencies with government agencies, public works, and transit agencies. The system will replace the patchwork of radio frequencies and incompatible equipment that have supported the region's emergency response operations. The system is designed to provide the portable mobile coverage that outdated systems cannot provide, and will address channel crowding issues.

Planning for the system has been extensive, with project working groups created in 1995. To drive progress, Junkins leverages best practices gleaned from neighboring municipalities, the Association of Public-Safety Communications Officials, and the National Emergency Number Association.

Ten-Codes: Over and Out?

The days of 10-codes—a second language for many police departments—may be numbered.

“Ten-codes are going into the history books just as the revolver did. The revolver was the most important tool in its day for law enforcement, but it has been replaced with a more effective tool—the semi-automatic pistol,” says Tom Chirhart, OIC Spectrum and Interoperability Technologies Program Manager. “And, like the revolver, 10-codes have made their mark in the history of public safety.”

In the 1940s, the Association of Public-Safety Communications Officials developed and later updated a standardized set of 10-codes. Today, however, the meaning of a set of 10-codes can vary from department to department—causing confusion during multi-agency and multi-jurisdictional emergency responses.

In the National Capital Region, for example, a routine traffic accident became a scene of chaos when a Maryland State Police trooper radioed in a “10-50” using the Montgomery County, Maryland Police Department radio system. To the Maryland State Police trooper “10-50” meant “traffic crash.” To an officer in Montgomery County—which had recently transitioned to plain language—however, “10-50” meant “officer down.”

“The use of different 10-codes makes it almost impossible for our public safety personnel to understand what is being communicated since most localities and agencies use different codes,” says Chris Essid, Commonwealth of Virginia Interoperability Coordinator.

Ten-codes were originally intended to benefit emergency response operations. Decades ago, radio airtime was a premium. The standardized use of codes allowed police officers to quickly and securely exchange information using limited radio space.

Today, technological advances are both enhancing the mission of emergency responders, and changing the landscape in which police officers operate. Policy and procedures—including the use of codes and signals—have not advanced at the same pace as modern capabilities. Digital radio technology has made more bandwidth available to police departments, and new digital radios with encryption allow for secure communications without the use of 10-codes. Moreover, the use of scanners to monitor emergency response communications, and the availability of code definitions on the Internet, compromise the security that 10-codes once ensured. Despite these factors, the majority of police departments nationwide still use 10-codes and signals.

But not all. Virginia Governor Tim Kaine’s ongoing effort to transition from 10-codes to the use of plain language is gaining momentum and support from many emergency response practitioners and organizations. Advocates of the shift point to communication breakdowns during recent disasters as impetus for change.

”The first responders [in Virginia] identified the need to move away from codes as the top interoperability priority in Virginia’s Statewide Interoperable Communications Plan”, says Essid. “This results from problems with 10-codes at events that include September 11, 2001, Hurricane Katrina, and other events prior to these.”

To drive the region’s transition from 10-codes to plain language, the Commonwealth of Virginia formed an Initiative Action Team (IAT) comprised of multiple emergency response agencies.

“The whole idea behind forming an IAT is to let the very people this change will impact the most, public safety responders, decide how to migrate so it is done right,” says Essid. “This was a nine-month process that included many meetings, conference calls, and emails to ensure the IAT considered almost every aspect of the transition.”

The IAT recommended use of plain language for all transmissions with the exception of four universal signals used to ensure responder safety.

Virginia’s transition has been endorsed by a number of emergency response associations and agencies, including the Virginia Fire Chiefs Association, Virginia Sheriff’s Association, Virginia Chapter, Association of Public-Safety Communications Officials, and the Virginia State Police (VSP). VSP Superintendent Colonel W. Steven Flaherty has been a key advocate of the transition from 10-codes to plain language. Under his leadership, the VSP, on October 1, 2006, switched to plain language—a significant step toward a statewide transition.

“Under the outstanding guidance and leadership of Colonel Flaherty, the VSP—which had a 30-year-old radio system, and a reputation among local law enforcement agencies as being resistant to change—has gone on to become an agency currently with the most advanced statewide radio system and one of the first state police agencies in the Nation to adopt this concept,” says Captain Eddie Reyes of the Alexandria, Virginia Police Department, who chaired the Virginia State Interoperability Executive Committee.

To assist the transition, new recruits at law enforcement academies and current officers will receive training in 10-codes. “One of the beautiful things about this transition is that it will take less training than it did for folks to learn their department’s 10-codes,” says Essid.

Reyes recalls the training required to learn his department’s set of 10-codes. “Our organization has 100 10-codes. As a new officer, I’d spend hours trying to memorize them. Today, new officers [at agencies using plain language] only have to memorize the four 10-codes used for officer safety.”

Advocates of plain language stop short of saying that Virginia’s transition is indicative of a national trend. Officers have used 10-codes for decades, and are comfortable with their verbal shorthand. In addition, without a universal set of plain language phrases, many see no reason to replace familiar 10-codes. Opponents to a transition also contend that plain language uses more air space than does “code-speak.”

However, says Reyes, “This [air space issue] is one of those plain language myths. For example, if you look at the time it takes to say ‘10-76’ versus the time it takes to say the plain language version [of 10-76]: ‘enroute,’ you can see that a 10-code is not always quicker than its plain language counterpart.”

Q&A With Jim Junkins

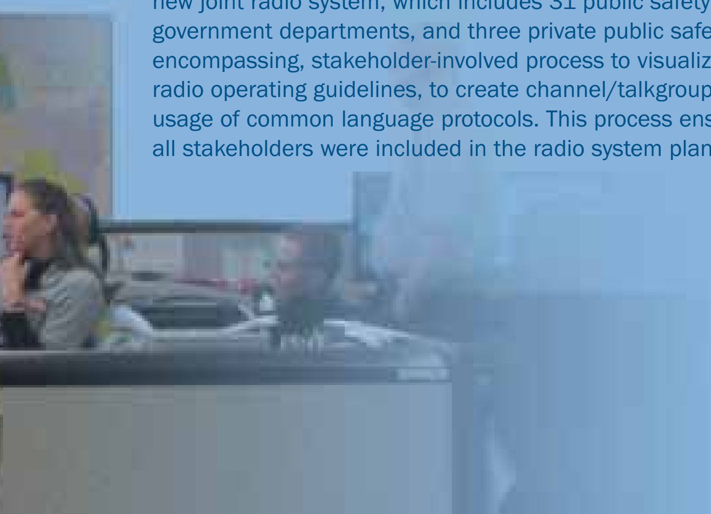
Q. In your view, what are today’s major challenges in interoperability?

A. The human element—including comprehension of interoperability needs and cooperation across disciplines and jurisdictions—is a top challenge. Many are only aware of interoperability because it’s today’s buzzword. Likewise, many perceive interoperability as only necessary for the terrorist attack or the large-scale natural disaster; they forget that interoperability is just as important for day-to-day events. A comprehensive understanding and acceptance of public safety’s need to interoperate every day—among disciplines, divisions, all levels of government, and the private sector—is critical to interoperability progress.

Q. What steps is HRECC taking to address this interoperability challenge?

A. The HRECC is only one component of emergency communications for the City of Harrisonburg and Rockingham County, Virginia. Identifying and bringing all stakeholders—local officials, policy makers, public safety responders—to the table is critical in order to ensure that everyone understands a locality’s comprehensive interoperability needs.

This stakeholder-driven approach has been key in successfully designing our new joint radio system, which includes 31 public safety agencies, all general government departments, and three private public safety entities. We utilized an all-encompassing, stakeholder-involved process to visualize the end result, to develop radio operating guidelines, to create channel/talkgroup plans, and to coordinate usage of common language protocols. This process ensured that the perspectives of all stakeholders were included in the radio system plan.



Q. How did you become interested in interoperability issues?

A. For many years, public safety responders have struggled with no or ineffective communications—often unable to talk to some parts of their own agencies, let alone communicate with agencies in neighboring jurisdictions or states. The communications needs I witnessed during my 26 years of volunteer firefighting coupled with my technical background first motivated me to look for means of fostering interoperability. Tragic events like September 11, 2001, have created opportunity for change and progress. This opportunity coupled with today’s technology possibilities drives me even harder to develop total interoperability solutions for public safety stakeholders.

Q. What lessons have you learned since becoming involved in the field?

A. When I first began this career, I believed that technical solutions would achieve interoperability. I, however, was forgetting the missing link: people and why they would not want to interoperate. I soon realized that the complexity of this challenge is far beyond that of sharing a radio channel. Turf wars go to the very root of interpersonal communications and the “virtual walls” that can exist between public safety disciplines.

Today, I strive to not only design technical interoperability solutions, but also to foster relationships and cooperation among disciplines and beyond. Interoperability, really, is 90 percent a people issue and 10 percent a technical issue.

Q. If you were not doing this type of work, what would you be doing?

A. I continue to be amazed at the human ability to expand and diversify technical innovations above and beyond the purposes for which they were originally designed. My current and past careers have been a mix of developing technical solutions to solve problems and enhance communications. I cannot imagine a career without those two components, as they equally intrigue and drive me.

Welcome to the Team

The Office for Interoperability and Compatibility (OIC) recently welcomed Denis Gusty and Luke Klein-Berndt to its team. Mr. Gusty leads many of OIC's non-technical initiatives, including stakeholder coordination and statewide planning efforts. Mr. Klein-Berndt is leading OIC's standards and technology efforts.

Mr. Gusty comes to OIC from the U.S. General Services Administration (GSA), where he served as Director of GSA's Office of Intergovernmental Solutions. Prior to joining GSA, Mr. Gusty served as a Program Manager at the U.S. Department of Labor. In this role, he was responsible for helping to implement the President's Management Agenda by managing the e-Government initiative, GovBenefits.gov. Mr. Gusty has more than four years of experience in developing intergovernmental partnerships and IT policy and practices.

Mr. Klein-Berndt brings more than five years of communications technology experience to OIC. Before joining OIC, Mr. Klein-Berndt worked in the National Institute of Standards and Technology's Office of Law Enforcement Standards. While there, Mr. Klein-Berndt specialized in interoperable communications, including Project 25. He has an extensive background in computer science.

2007 INDUSTRY ROUNDTABLE

The Department of Homeland Security's 2007 Industry Roundtable takes place May 9-10 in Washington, DC. The Roundtable will bring together emergency response leaders, industry representatives, and government officials to collaboratively address key interoperability challenges.

Roundtable discussions include: findings from the National Interoperability Baseline Study; grant guidance; Project 25 and the Compliance Assessment Program; Voice over Internet Protocol; broadband; data networks; and the National Information Exchange Model. These discussions support interoperability progress by building essential partnerships and helping industry align technology solutions with emergency response needs.

To see the full agenda, or to register for the Roundtable, please visit www.safecomprogram.gov or http://oic.csrincorporated.com.

Interoperability Technology Today

Homeland Security

A Resource For the Emergency Response Community

Spring edition 2007

"This edition features . . ."

- Lessons learned from interoperability initiatives in Dallas, Texas
- A look at law enforcement interoperability needs and approaches to progress
- Success stories from Disaster Management's Standards Working Group
- Trends in 10-code and plain language usage nationwide
- Best practices from Jim Junkins, Director of Virginia's Harrisonburg-Rockingham Emergency Communications Center
- An overview of the Interoperable Communications Technical Assistance Program

Office for Interoperability and Compatibility
Science and Technology Directorate
U.S. Department of Homeland Security
Washington, DC 20528