



Interoperability TECHNOLOGY Today

A Resource for the Emergency Response Community

Summer 2007



LAST FRONTIER STATE ACHIEVES INTEROPERABILITY "FIRSTS"

If it was possible to see one square mile of land in one minute, it would take one hour to see the District of Columbia. It would take one day to see the State of Rhode Island. And, it would take one year, one month, and one week to see the State of Alaska.

The vastness of Alaska's land mass coupled with its small population—650,000 full-time residents—presents the region's emergency responders with significant challenges. Because the state's infrastructure is disproportionately small compared to its land mass—there are fewer paved roads in Alaska than there are in the State of Vermont—the mobility of emergency responders is restricted. Hundreds of communities can only be reached by sea or plane. Often, high winds, storms, and poor visibility compromise responder safety and operations, delaying emergency response by hours—sometimes even days.

Many communities are as removed from electrical systems as they are from state highways. Without access to reliable communications, manageable incidents are more likely to escalate into large-scale emergencies. These challenges are complicated by the fact that an estimated 50 percent of Alaska's land mass does not have local or county governments—obligating state and emergency response agencies to provide local services.

"Without local or county governments, communities operate under the direct services and provisions of the state," says John Madden, Director of the State of Alaska's Division of Homeland Security and Emergency Management. "This puts a great deal of responsibility on response agencies, like the National Guard, Alaska state troopers, and Alaska Division of Homeland Security and Emergency Management, to coordinate local emergency response from the state and Federal levels. It also complicates planning with our Federal partners, such as Federal Emergency Management Agency, Department of Defense, and law enforcement agencies."

With a limited supply of personnel and resources, partnerships, collaboration, and resource sharing are critical to the success of Alaska's emergency response operations. Local, tribal, state, and Federal representatives routinely partner through consortiums intended to address day-to-day complexities. These consortiums have supported Alaska's commitment to strengthening statewide emergency response. To meet the emergency response needs of its most remote localities, Alaska has developed programs to provide these regions with satellite phones to communicate with operation centers, as well as training to manage emergencies until responders arrive.

Impetus for Change

While Alaska's leaders have long understood the importance of interoperability, the issue topped agendas in June 1996 after communications breakdowns compromised local response operations during a large-scale fire in the Matanuska Valley. The magnitude of the blaze demanded a multidiscipline, multijurisdictional response—including the National Guard, fire response, and law enforcement agencies. When responding agencies arrived on-scene, they discovered that their radios were incompatible.

"In order to communicate," Madden recalls, "responders had to physically swap radios. It wasn't uncommon to see an incident commander with five radios hanging from his belt."

Interoperability progress in Alaska gained momentum in 1997 when, in response to the Matanuska Valley fire, the Alaska Land Mobile Radio (ALMR) Executive Council initiated a collective planning process to address interoperability for emergency response agencies across all levels of government. Originally formed in 1995 to address the state's migration to narrowband operations, the ALMR Executive Council represents Alaska's commitment to cross-government partnerships. The council's four charter members included a local representative, a state representative, a Federal civilian representative, and a Federal military representative.

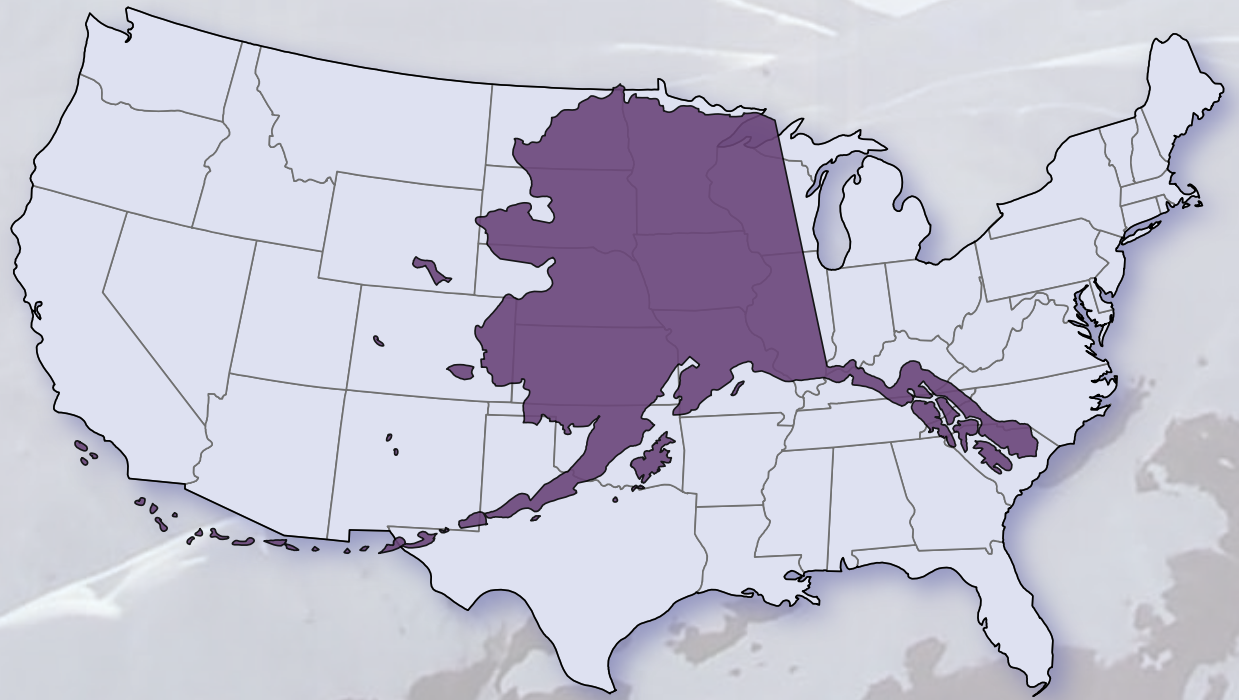
Today, the ALMR Executive Council functions as Alaska's State Interoperability Executive Committee. Council members represent emergency response needs of local, tribal, state, and Federal governments, as well as industry. To ensure that statewide interoperability planning incorporates the input of responders on the frontlines, the ALMR Executive Council established a User Council. Comprised of emergency response representatives with extensive field experience, the User Council offers recommendations to the Executive Council.

Comprehensive Connectivity

The state's collaborative approach to advancing interoperability has proven invaluable in successfully implementing the ALMR System, a statewide, interoperable, trunked radio system connecting 40 agencies.

"One of the distinctive elements of this system is that it enables interoperable communications across the entire spectrum of government—local, state, Federal military, and Federal civilian," says Madden. "Our police, fire, and emergency medical service responders can communicate with our military—that's unique." And important. With a high demand for mutual aid operations, effective coordination between Alaska's emergency response agencies and the military is critical.

continued on page 6



To-scale map of Alaska superimposed on the Nation's lower 48 states.

CONTENTS

Last Frontier State Achieves Interoperability "Firsts" . . .	1
Director's Message	2
Disaster Management Scores Touchdown at Super Bowl XLI	3
Roundtable Dialogue Marks Milestone in Industry Partnership	3
800 MHz Rebanding a Spectrum of Lessons Learned at Two-Year Anniversary	4
OIC Releases Shared Channels Planning Guide	5
In Your Own Words	6
Spotlight on Chief Jeff Johnson	7

Lessons Learned from Interoperability Progress in Alaska

- Recruit leaders to the interoperability effort who have extensive field experience. These leaders will understand the broader impact of policy and strategy decisions on responders in the field.
- Involve emergency response frontline users early on. Practitioner input and investment are critical to a successful initiative.
- Address interoperability challenges with a multidimensional—not linear—approach. Interoperability elements—standard operating procedures (SOPs), technology, training, equipment, governance—are interdependent. It is important to make movement across all of these elements simultaneously. Thus, before implementing an operations system, develop SOPs for regional coordination.
- Standardize where possible, customize where necessary. Where things are alike, use the like solution, where things are different, customize solutions to meet specific needs.



Interoperability About 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 preparedness and response. 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 programs address both voice and data interoperability. OIC 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. OIC is also improving incident response and recovery by developing tools, technologies, 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, visit www.safecom.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 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 summer 2007 edition of *Interoperability Technology Today*, published by the Department of Homeland Security, Office for Interoperability and Compatibility," should be included.

Photo Credits: Photos and graphics used in this edition of *Interoperability Technology Today* include images from Stock.XCHNG, FreeRange Stock, and Getty Images.

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

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>

International Association of Chiefs of Police 114th Annual Conference & Exposition

October 13-17, 2007
New Orleans, Louisiana
www.iaacp.org



DIRECTOR'S MESSAGE

By Dr. David Boyd

Since its early days, the Office for Interoperability and Compatibility (OIC) has been committed to improving voice interoperability—considered by emergency responders to be the most fundamental and crucial communication mode among dispatchers, command, and field responders.

Today, the ability to exchange emergency data—a map, video image, situational report, hospital bed availability—is increasingly critical to the success of emergency response operations. In response to practitioners' data interoperability needs, OIC launched an initiative intended to identify ways to integrate data considerations into its voice interoperability resources.

This "integration study" revealed that while the technical aspects of voice and data interoperability issues may differ, many challenges to achieving seamless communications—incompatible proprietary systems, ineffective governance—overlap.

As a result, OIC's data efforts benefit from much of the Office's voice-focused work—including field pilots, architecture frameworks, standards acceleration, and the development of replicable tools.

Similarly, the practitioner-driven approach that has been at the heart of OIC's work is yielding significant success across its work in data. In fact, many of the practitioners that contribute to OIC's voice-centric working groups also contribute to its data-centric working groups.

The integration of voice and data resources supports a holistic approach to interoperability—advancing OIC's ability to effectively address all aspects of interoperability.

OIC has integrated a number of tools, including:

- Creating a Charter for a Multi-Agency Interoperability Committee: Template and Questions to Consider—Governance is a universal requirement for voice and data communications interoperability. While many communities have the technology to interoperate within their own or neighboring jurisdictions, they often lack the resources to develop and support a governance structure. Practitioners working with both voice and data communications may thus require charters to aid in the establishment of multi-agency interoperability committees.
- Statewide Communications Interoperability Planning (SCIP) Methodology 2.0—Statewide planning for and implementation of voice and data systems bear many similarities, and are typically carried out simultaneously in a coordinated effort. Integrating this tool has increased the SCIP Methodology's applicability and scope.
- Statewide Planning Guidebook—States are required to develop strategic plans for communications interoperability by November 2007. This Guidebook helps states ensure that their plans address both voice and data considerations.

OIC is committed to a forward-looking approach for the development of tools—ensuring that resources take into account all aspects of interoperability. As always, practitioner needs will drive the design and development of these tools. We look forward to continuing to work with the emergency response community and Federal partners to equip localities with the resources to navigate the road to interoperability.

Disaster Management Scores Touchdown at Super Bowl XLI

From instant replay to helmet radios, communications technology is an increasingly important playmaker in the Super Bowl. At this year's Super Bowl XLI, the Disaster Management (DM) program's Open Platform for Emergency Networks (OPEN) scored a touchdown *off* the field.

Played on February 4 in Miami Gardens, Florida, this year's Super Bowl drew more than 200,000 loyal Chicago Bears and Indianapolis Colts fans to Dolphin Stadium. Ensuring the safety of players and fans at the highly visible event required the support of multiple organizations. These included the Miami-Dade County emergency response departments, the United States Secret Service, the Federal Bureau of Investigation, and chemical and biological response teams. The ability of these organizations to successfully share information across multiple systems and devices was essential.

The need for data exchange, coupled with the involvement of multiple organizations, provided DM with an opportunity to field-test OPEN. OPEN is a non-proprietary, operational interoperability backbone that allows disparate, third party applications, systems, networks, and devices to securely share information.

At Super Bowl XLI, OPEN was deployed with the Department of Homeland Security's (DHS) Biological Warning and Incident Characterization (BWIC) system in order to simulate a chemical and biological data exchange. This was the first time the systems had been simultaneously deployed. The BWIC system is designed to help public health and emergency management officials prepare for and respond to biological terrorist attacks and to certain public health threats. Developed in response to local and state requests, BWIC provides integrated decision support to assist timely warning, attack assessment, communications, and effective response in the event of a biological attack.

OPEN allowed BWIC to share the data it had generated with multiple emergency response systems and devices. Sharing was enabled through DM's Common Alerting Protocol (CAP) standard. Had a hazardous bioagent actually been detected, emergency response organizations supporting the Super Bowl would have received alerts. The simulation—about which spectators were unaware—demonstrated that systems can effectively share data if they adhere to standard protocols for incident reporting and collaboration.

Characterized as a success by Miami-Dade County emergency responders, the field test was a milestone for OPEN—demonstrating its viability for nationally significant, high-profile events like the Super Bowl.

Building on their success at Super Bowl XLI, OPEN and BWIC were deployed in support of the Air & Sea Show, held in Miami, Florida last May. OPEN and BWIC were used to send CAP alerts to various text-enabled wireless phones. OPEN was used to show the status of the event, from its initial stages through the end of the show.

For more information about BWIC, visit: http://www.sandia.gov/mission/homeland/factsheets/new06/BWIC_factsheet.pdf.
For more information about OPEN, visit: <https://www.disasterhelp.gov/suite/>.

Open Platform for Emergency Networks (OPEN)

DM's OPEN is a non-proprietary, operational interoperability backbone that allows disparate third-party applications, systems, networks, and devices to securely share information.

OPEN provides:

- An infrastructure with common service functions that enable different automated information systems to exchange data.
- An interoperable platform to assist vendors with prototyping, testing, and implementing emerging data standards.
- A highly secure environment in which the emergency responder community can share data with whom it wants when required.

OPEN is deployed on a national level—enabling incident management software, applications, and devices at all levels of government to share information through a secure, open architecture platform.

OPEN is available to members of the emergency response community at no cost. DHS provides emergency response agencies and vendors who develop emergency related software with OPEN network management and technical support. System or software compatibility is not an issue; participating systems conform to the shared interface standards when conducting transactions. This allows organizations to make changes to a system without affecting the ability to share information with other systems.

All upgrades to increase data sharing capabilities are free for emergency responders. To register for OPEN, visit www.DisasterHelp.gov.

Roundtable Dialogue Marks Milestone in Industry Partnership

On May 9-10, emergency response leaders, industry representatives, and policy makers took a significant step toward aligning interoperability technology solutions with the needs of practitioners in the field. These leaders, and more than 250 local and state emergency responders, convened in Washington, DC for the Office for Interoperability and Compatibility's (OIC) 2007 Industry Roundtable. The theme was: "Working together to create a 'system of systems' to support emergency response communications interoperability." This Roundtable provided a valuable forum for stakeholders to collaborate on critical interoperability technology challenges.

Building on the successes of last year's inaugural Industry Summit, this year's OIC progress report on interoperable communications emphasized the need for emergency responders, industry, and policy makers to engage with each other on interoperability issues.

"The 2007 Industry Roundtable provided a great opportunity for emergency responders to meet with industry and discuss the technical needs of the emergency response community. OIC is to be congratulated for providing such an opportunity to help strengthen interoperability," says Kevin McGinnis, Communications/Technology Advisor, National Association of State Emergency Medical Services Officials.

In keeping with the event's emphasis on stakeholder engagement, OIC designed Roundtable sessions to encourage active dialogue among participants. Interactive panel sessions and question-and-answer periods allowed interoperability field experts to engage with participants on a wide spectrum of matters. Speakers included the Department of Homeland Security's (DHS) Science and Technology Directorate Under Secretary Jay Cohen, Congressman Dave Reichert, Ranking Member on the House Homeland Security Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, and Congressman Bennie Thompson, Chairman of the House Homeland Security Committee.

"The discussion between the public safety community and industry at this year's Industry Roundtable was fruitful for both groups," says Andrew Thiessen of the National Institute of Standards and Technology/Office of Law Enforcement Standards. "Both sides had an opportunity to talk about key issues from their different perspectives, and continue to build the critical partnership necessary to achieve communications interoperability. This partnership will continue to reap benefits for the Office's technical initiatives."

continued on page 6

Running Interference: Why Reconfigure the 800 MHz Band?

Emergency response systems operating in the 800 Megahertz (MHz) band have experienced increasing levels of interference and dead zones. This interference occurs because emergency response systems use a fundamentally different system architecture than do the commercial wireless systems operating in nearby spectrum.

For many years, emergency response radio systems operated in the 800 MHz band with occasional harmful interference. The original band plan did not anticipate the development and accelerated growth of the commercial wireless carriers using 800 MHz, cellular-type, architecture systems.

Emergency response systems traditionally use a single base station with a high antenna in a favorable location, within the desired coverage area. The transmitted signal is strongest near the base station and loses strength the farther away it is from the base station. Emergency response systems use receivers that can receive relatively weak signals.

Conversely, commercial wireless carriers typically accommodate large volumes of communications traffic by using a “cellular-type” architecture. This architecture consists of a large number of base stations, using relatively high power, but relatively low-site antennas in order to limit coverage to a small area around that base station.

Over time, 800 MHz emergency response radio systems became more widespread, and commercial wireless systems experienced a dramatic increase in subscribers resulting in more vigorous reuse. This involved a greater number of cell sites and a greater number of frequencies in use at those cells. As a result, emergency response users began to encounter pockets of “dead zones” within their coverage areas, where the signals from commercial wireless systems overwhelmed the sensitive emergency response receivers.

Sprint Nextel has created a three-person emergency response advisory board that is designed to provide the wireless carrier with additional insight into the views of emergency response licensees participating in the rebanding of 800 MHz spectrum. The panel is also designed to provide a function of outreach between emergency response agencies and Sprint Nextel. Advisory board members are Stephen Browne of Denver, Colorado, David Seidel of San Bernardino, California, and Charles Werner of Charlottesville, Virginia. If members of the emergency response community wish to contact these advisory board members, they may email them: David Seidel at daseidel@verizon.net, Stephen Browne at scbrowne@att.net, and Charles Werner at werner@charlottesville.org.

800 MHz REBANDING A SPECTRUM OF LESSONS LEARNED AT TWO-YEAR ANNIVERSARY

The emergency response community and the Federal Communications Commission (FCC) recently passed the two-year mile marker for the 800 Megahertz (MHz) rebanding process.

Initiated in June 2005, this rebanding process addresses increasing levels of life-threatening interference and dead zones experienced by emergency response systems operating in the 800 MHz band. To prevent radio system interference from commercial carriers, the reconfiguration separates spectrum for private cellular carriers from spectrum for emergency response systems. Separating these communications requires moving emergency response systems to spectrum lower in the 800 MHz band, and moving commercial carriers, such as Sprint Nextel, to the opposite end of the band.

“This is an incredibly complicated nationwide program that has never been attempted before,” says Brett Haan, Deputy Program Administrator, 800 MHz Transition Administrator (TA).

Multiple Players

The success of this massive rebanding process requires commitment and coordination across a diverse group of stakeholders. While the FCC ordered the reconfiguration, an independent entity appointed by the FCC, the TA, manages the reconfiguration process. The TA: 1) oversees the administrative and financial aspects of the band reconfiguration; 2) provides accountability; and 3) ensures that band reconfiguration is achieved with minimal disruption to licensees.

The commercial carrier Sprint Nextel is reorganizing within the band in exchange for other spectrum. The carrier is responsible for the cost of relocating all affected 800 MHz users to new spectrum with facilities comparable to those presently in use. Finally, emergency response agencies and associations—the drivers of the rebanding change—are heavily involved in the rebanding process. They are reprogramming units, maintaining interoperability, budgeting, negotiating, and collaborating across disciplines, jurisdictions, and regions.

Utah Communications Agency Network (UCAN) Executive Director Steve Proctor relates that the UCAN radio system operating in the 800 MHz frequency band serves 130 emergency response agencies statewide. It is responsible for 12 counties and 85 percent of Utah’s 2.4 million-plus population. “This is a huge process,” Proctor says. “We have to educate the 130 government entities we serve, reprogram 16,000 subscriber units—which are not in a central location but must be brought into a central depot—and, while we’re doing all this, we need to ensure continuing interoperability. It’s as if we’re remodeling our home,” he adds. “We’re moving walls but we’ve got to keep the roof on and live in the house while we do it.”

With the reconfiguration’s complexity comes a variety of challenges, including important implications for interoperability.

Impacts on Interoperability

The 800 MHz reconfiguration is implemented across the Nation in four “Waves.” Wave sets are based on groupings of the 55 National Public Safety Planning Advisory Committee regions. Each Wave contains groups of regions that will begin rebanding at the same time. Rebanding start times are staggered by Waves across the Nation.

Some regions—such as Virginia’s Hampton Roads region and North Carolina—operate in close proximity, but will reband at different times. Some stakeholders worry that different rebanding timelines could compromise interoperable communications.

Rebanding processes within Waves also may impact interoperability. For example, Wave One encompasses many heavily-populated urban areas in which agencies regularly communicate across jurisdictional lines—using long-established interoperability plans. Reprogramming the hundreds of thousands of radios used by these agencies is a complicated and lengthy task; not all agencies will be ready to reband at the same time.

“I have a concern that the rebanding effort is occurring by individual licensees and not by the region. Some regions have robust interoperability solutions in place in the 800 MHz band that are now threatened by rebanding by licensee,” says Office for Interoperability and Compatibility Spectrum Manager Tom Chirhart. “Unless the rebanding is done by region, for those regions with a robust interoperability solution, there is a potential for serious disruption or degradation of the legacy interoperability capability.”

Critical Coordination

Regional coordination is critical to supporting legacy interoperable capabilities throughout the rebanding process.

Brad Barber, Senior Consultant for a Virginia-based engineering firm supporting the project, offers “four W’s” to consider for interoperability coordination during rebanding:

Who: Who do you talk to and who needs to talk to you? Don’t forget to include non-traditional emergency response entities like hospitals or nuclear facilities, in addition to those emergency response and mutual aid agencies that may come to you from out of the area during emergencies.

What: What channels and talk groups do you use? What types of equipment, and what are their technical limitations? As the actual rebanding process begins, which may take months or years to complete, how does an agency maintain its ability to communicate? For example, some radios don’t have enough memory to program both the old and new channels during the process. Don’t forget the need to reprogram gateway devices.

When: Multiple agencies have multiple schedules, and the pace of negotiations and official sign-off by all parties involved is slow.

Where: You have to ensure your systems have comparable radio coverage before, during, and after the reconfiguration. Your plan must include the fact that you may have to stop rebanding in the middle to respond to an event like a hurricane. Can you still communicate?

Reconfiguration Costs and Negotiations

The unprecedented and highly complex nature of the 800 MHz rebanding process presents agencies and vendors with exceptional planning and budgeting challenges. “We feel like we’re inventing the process as we go along,” says Proctor.

Reconfiguring 800 MHz licensees, including emergency response agencies, are required to negotiate the specifics of their reconfigurations directly with Sprint Nextel. According to the TA, as a Wave begins rebanding, a Sprint Nextel representative will contact licensees in that Wave to start

negotiations to complete a Frequency Reconfiguration Agreement (FRA), and/or a Planning Funding Agreement (PFA).

A PFA is required if a licensee requires reconfiguration planning funding, e.g., for inventories, frequency evaluation, development of cost estimates. The PFA is used as input to the cost estimate, and the FRA negotiated with Sprint Nextel. Issues with PFA approval can lead to stalled negotiations and TA mediation, known as Automatic Dispute Resolution (ADR). Mediations are initiated for matters both complex and straightforward, that is, from cost disagreements to late signatures. If the matter is not resolved at the completion of the ADR process, the TA refers the matter to the FCC.

“The mediation process can be very lengthy,” says Robert Gurs, Director of Legal and Government Affairs for the Association of Public-Safety Communications Officials-International, Inc. Gurs is an attorney who has represented emergency response agencies in the negotiation process. “The mediators are mostly commercial lawyers who did not know telecom initially, and who had not dealt with this level of radio detail. There’s been a learning curve, and the process has improved.”

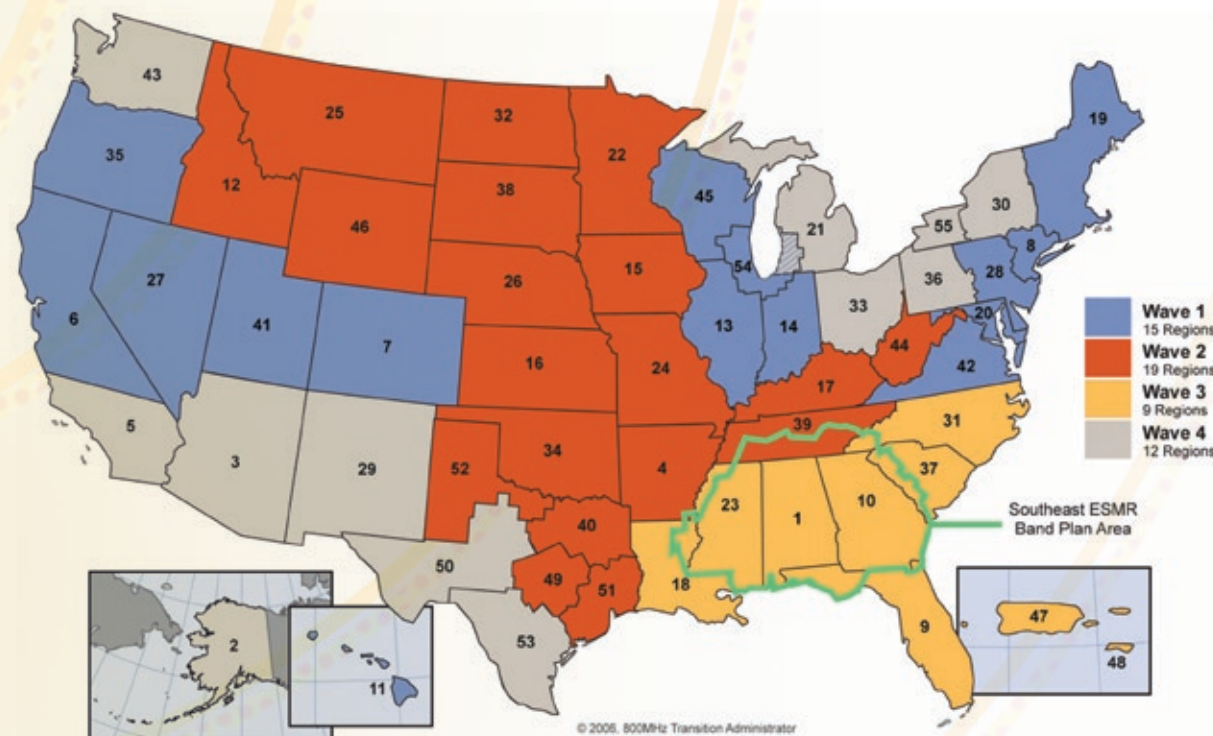
In January 2007, the FCC ruled that emergency response agencies engaged in rebanding can share information among each other on the terms of their negotiations with Sprint Nextel. A win for the emergency response community, the ruling supports good-faith negotiations and advancement of the reconfiguration process.

“The FCC’s recent order allowing agencies to disclose or exchange information between licensees on their negotiations is going to go a long way to helping public safety,” says Chirhart. “We have always advocated the sharing of lessons learned. Those who have already gone through this process already know what is involved in the preparation for negotiations and how to avoid pitfalls. Their sharing will assist other public safety agencies navigate through the various stages of reconfiguration.”

A massive and complex “learn-as-you-go” task, the 800 MHz rebanding has met its share of obstacles. Fortunately, the flexibility of the rebanding process has enabled the initiative to respond to challenges, incorporate lessons learned, and prepare for the steps ahead.

To assist emergency response leaders address reconfiguration and related interoperability issues, the TA has several resources available on its Web site at www.800ta.org.

For more information about the 800 MHz reconfiguration, contact the TA by phone at (888) 800-8220, by fax at (888) 701-4380, or by e-mail at comments@800TA.org.



FROM SIMULATION TO FORMULATION: BROADBAND STANDARDS AT A GLANCE

When the Federal Communications Commission allocated 50 Megahertz (MHz) of spectrum in the 4.9 gigahertz (GHz) band in 2002, emergency responders nationwide gained access to technology and application capabilities previously available only to commercial wireless users. The band’s suitability for high-speed data transmission enables responders to implement advanced on-scene services—including streaming video and emergency data exchange, missing person images, situational maps, and medical files. The 4.9 GHz allocation also gives every jurisdiction across the Nation access to all 50 MHz of spectrum intended for interoperable broadband communications.

This unprecedented allocation brought with it a need for broadband standards development. What open standards need to be developed or modified so that technologies operating in the band are inherently interoperable, and successfully meet the needs of responders in the field?

Today, the Broadband Task Group (BBTG), of the Association of Public-Safety Communications Officials-International Project 25 Interface Committee (APIC), is working with emergency responders to drive broadband standards development. The BBTG leverages existing broadband standards—those designed for commercial technologies—by simulating complex communication transfers used during emergency events.

To simulate these transmissions, the BBTG uses a computer software program to model an emergency incident environment. Emergencies are based on the practitioner-defined scenarios—heart attack, house fire, traffic stop, chemical plant explosion—in the *Public Safety Statement of Requirements for Communications & Interoperability, Volume I, v1.0*. Emergency responders assist the BBTG in accurately capturing operational factors that affect emergency communication transfers—including message content, transmission timeframes, and position of responding vehicles and command posts.

Once the emergency environment is modeled, the BBTG simulates the communication transmissions to analyze the performance of existing and emerging technologies. Results from these simulations help determine gaps between the performance of the technologies and the comprehensive requirements for voice, data, video, and other application data in near-future emergency environments. The results also provide recommendations for transmission protocol changes to develop emergency, responder-grade, interoperable broadband standards.

The APIC BBTG’s standards development work represents a significant step toward ensuring that emerging technologies successfully meet the needs of emergency responders on the ground.

For more information about the BBTG and its work, please contact Andrew Thiessen, BBTG Chair, at athiessen@its.bldrdoc.gov.

OIC Releases Shared Channels Planning Guide

The Office for Interoperability and Compatibility (OIC) has released the *Improving Interoperability Through Shared Channels* planning guide. Designed for emergency response leaders at all levels of government, this guide outlines the key actions and considerations necessary for the development and implementation of a shared channel solution for communications interoperability. Because it requires limited resources and leverages existing systems, the shared channel solution can help emergency responders inexpensively achieve improved cross-discipline and cross-jurisdictional interoperability. OIC is developing supporting resources that will document nationwide examples of successful shared channel solutions. *Improving Interoperability Through Shared Channels* can be found at www.safecomprogram.gov.



Alaska • continued from page 1

The ALMR System replaces outdated radio systems with a Project 25 standards-based system for integrated voice and data. It supports interoperable communications for events ranging from day-to-day operations to large-scale mutual aid operations. To leverage existing systems, the ALMR System is backward-compatible—allowing a radio to operate on both its existing system and the ALMR System. System infrastructure is cost-shared among state and Federal governments; thus, the ALMR System is a shared system both operationally and financially.

The ALMR System was put to the test in May 2007 during the Alaska Shield/Northern Edge exercise. A challenging, full-scale preparedness exercise, Alaska Shield/Northern Edge tested, in part, the ability of local, state, and Federal agencies to effectively share emergency information and coordinate tactical responses at 10 venues across 100,000 square miles, against simultaneous threats from air, sea, and land.

Making Strides

With the ALMR System operational in regions, Alaska is striding beyond the patchwork of frequencies and equipment that once supported the region's emergency response operations. "Today, a state trooper driving hundreds of miles along a state highway can communicate with every law enforcement agency along the way. That's a great achievement for us," says Madden.

Steven Covey's *Seven Habits of Highly Effective People* may hold truths for statewide interoperability planning, Madden notes. "To borrow from Covey, begin with the end in mind," says Madden. "Like a painter, you must have a design and vision in order to achieve the bigger picture. Understand how the steps you are taking today benefit the citizenry, and support your end goals."

Roundtable Dialogue • continued from page 3

The Roundtable agenda featured a variety of breakout sessions on matters that are topping the agendas of emergency response and industry leaders nationwide:

- "Grant Guidance: What You Need to Know" increased understanding of FY 2007 interoperable communications grant guidance among industry and stakeholders. The session provided an opportunity for industry representatives to provide input on how to improve the grant guidance process.
- "Emergency Interoperable Standard Efforts" clarified the purpose and values of standard development efforts; explored how the Federal Government, emergency responders, and industry can contribute; and discussed the status of standards adoption and implementation.
- "Voice over Internet Protocol (VoIP): What It Can Be" explained the potential roles of and opportunities for VoIP in the emergency response field, and highlighted the importance of collaboration in strengthening VoIP interoperability.
- "National Interoperability Baseline Survey: So What?" considered the implications and results of the Baseline Survey, and discussed solutions to gaps based on product-independent partnerships among industry and stakeholders.
- "Public Safety Broadband: Can It Really Work?" explored the opportunities, challenges, and implications of emergency response broadband for both industry and practitioners.
- "Project 25 (P25) Compliance Assessment Program (CAP): What Does It All Mean?" established a shared understanding of P25 CAP, progress to date, and the impact of CAP on P25 standards. The session allowed participants to discuss the implications of P25 CAP for grant guidance.

Through its interactive sessions, the 2007 Industry Roundtable generated the following accomplishments:

- Acknowledgment and identification of emergency response and industry interoperability progress to date
- Mutual clarity about operational restrictions and requirements of emergency response, industry, and the Federal Government
- Increased options for interoperability solutions that are affordable, workable, and based on the system of systems framework
- Commitment from emergency response, industry, and the Federal Government to lead follow-up collaborative events, and to continue the discussions initiated during the Industry Roundtable

An important milestone in interoperability progress, this year's Roundtable enabled emergency responders to communicate their requirements to industry, and enabled industry to provide emergency responders with an understanding of how it will align emerging technologies with interoperable communications requirements.

"We are pleased that there was an increased awareness among policy makers and participants of the unique complexity of the issues of interoperable communications in the emergency response environment," says Dr. David Boyd, Director of the Command, Control and Interoperability Division at DHS. "We believe that the Industry Roundtable has served as an important step in achieving nationwide interoperability."

More information about P25 standards progress is available at the P25 Technology Interest Group official Web site at <http://www.project25.org>.

IN YOUR OWN WORDS

By Marilyn Ward, Executive Director, National Public Safety Telecommunications Council

NAVIGATING THE STATEWIDE INTEROPERABILITY PLANNING PROCESS

Last March, the National Public Safety Telecommunications Council joined the National Governors Association, the Office for Interoperability and Compatibility, and emergency response representatives from across the Nation for a Statewide Planning Workshop. A milestone in nationwide statewide interoperability planning, this gathering generated a valuable cross-pollination of ideas. I returned to South Carolina with a notebook packed with scribbles—success stories from Utah, lessons learned from Florida, anecdotes from New Mexico, best practices from New York, and advice from the Virgin Islands.

Nearly five months later—with the 2006 Homeland Security and Public Safety Interoperable Communications grant program's November 1, 2007 deadline for statewide plans fast-approaching—we are entrenched in the statewide interoperability planning process. Even when it is organized in a spiral-bound guidebook, this process can seem overwhelmingly complex.

Leveraging best practices and lessons learned gleaned from the field is indispensable in navigating the multiple dimensions of statewide planning. Exchanges last March and in prior years reveal common denominators for successful statewide planning initiatives. The practices and approaches that follow are advancing progress in regions of all shapes and sizes.

Develop a statewide planning process that is user-driven and champion-supported.

In order for a statewide plan to effectively meet the interoperability needs of a region, it is critical that key stakeholders—emergency responders, policy makers, associations, industry, operations decision-makers—actively participate in the planning process. It is important to develop a process that is locally driven and champion-supported. A political champion can be an important agent for change—giving an interoperability initiative the momentum it needs to achieve end goals.

Establish a common vision for interoperability.

A shared vision for interoperability is essential to an actionable statewide plan. A shared vision provides statewide planning participants with "the big picture"—giving context for near-term decisions and solutions, and ensuring that actions are in support of a common end goal. It is important not to lose sight of the vision when we are up to our elbows in planning.

Think regionally.

Partnerships are critical to the success of interoperability progress. Regional collaboration is important, as large-scale emergencies often necessitate multijurisdictional responses. Creating an environment that encourages participants to hang egos and badges at the door will facilitate collaborative efforts. Many localities have found that regional preparedness exercises and training events help establish regional standard operating procedures (SOPs), and solidify relationships between responders. Regionally recognized codes for special emergency situations also have proven successful in some states.

Address interoperability comprehensively.

While a statewide plan may compartmentalize interoperability elements on paper, recognizing the interdependency of governance, technology, SOPs, training and exercises, and usage is key to making progress. A comprehensive approach to interoperability simultaneously addresses these elements. For example, a region that procures a new technology should plan training, and conduct exercises, to maximize use of the technology.

Maintain open communication channels.

Many times, regions limit planning participants to discussions during statewide planning sessions and formal meetings. However, open communication channels are important throughout the statewide planning process. Regular communications—e-mails, newsletters, bulletins—between meetings keep participants informed of progress, provide an opportunity to incorporate everyone's input real-time, and maintain users' investment in the process.

Build a statewide planning process with elasticity and endurance.

Strengthening interoperability is an ongoing process—not a one-time investment. A living document, a statewide interoperability plan needs elasticity to adapt to new communications needs and factors, such as emerging technologies and protocols. Also important is a planning process's staying power. November 1, 2007 represents a mile marker—not a finish line—for statewide interoperability planning. Interoperability planning will continue to be ever-critical as we work to meet the needs of today and prepare for the challenges of tomorrow.

Additional information about statewide planning is available at: <http://www.safecomprogram.gov/SAFECOM/statewideplanning/>

DRIVING PROGRESS IN OREGON

After more than 25 years in the fire service—12 years of which have been spent as a fire chief—Chief Jeff Johnson is no stranger to the interoperability challenges that face responders on the frontlines. Today, Chief Johnson is Fire Chief and Chief Executive Officer of Tualatin Valley Fire and Rescue. His fire department serves more than 420,000 residents across nine cities and three counties in the metropolitan area west of Portland, Oregon. Thanks in part to Chief Johnson's leadership as the Chair of Oregon's State Interoperability Executive Council (SIEC), the region is making major strides in interoperable communications.

"It amazes me that there has been a national standard for fire hose connections for four generations, but that the Nation has only just recently come to a place where communications standards are expected," says Chief Johnson, a member of the Office for Interoperability and Compatibility's Emergency Response Council. "In our jurisdictions, we have standardized our cross-discipline voice communications systems. Today, talking to police and transportation officials in our own and neighboring jurisdictions is as simple as changing the channels."

In the metropolitan area, local agencies are partners in multidisciplinary emergency response communications—all using interconnected 800 MHz radio systems and

networking within and between the metropolitan counties and cities. A champion of collaborative approaches, Chief Johnson credits this progress to cooperation and resource sharing across agencies.

In his role as the SIEC Chair and President of the Western Fire Chiefs Association, Chief Johnson draws on his locally-driven approach and field experience to drive progress well beyond the borders of the metropolitan area. Recognizing that emergencies know no boundaries, Chief Johnson is assisting with important partnerships across diverse stakeholder groups—many with competing constituencies and agendas.

This type of leadership and collaboration, Chief Johnson says, is critical to improving voice and data interoperability. "You can't achieve progress without a common vision," he says, "and this requires good leadership and healthy collaboration."

"My job is to get a diverse group of people to work toward a common vision and an understanding of the challenges at hand—big price tags, uninformed policy makers, and incompatible systems. By staying focused on the finish line—our vision for interoperability—we're better able to overcome the obstacles on the way there."



Q&A with Chief Jeff Johnson

Q. In your view, what is one of the Nation's top interoperability needs?

A. A lack of interoperability exists at all levels of communications—especially for mission-critical communications. We need a national vision for interoperability. As the public safety community drives progress in localities and across regions, we need to know what the top of the puzzle box—the national vision—looks like so that we know how to connect our individual pieces; that is the only way we will end up with a complete picture of interoperability.

Q. What are the major technology challenges facing emergency responders nationwide?

A. Operability is as much of a concern as is interoperability. Aging, inadequate, and disparate systems lack security, reliability, and survivability. Today in Oregon, we're patching together some older radio systems that require parts that are even no longer available on eBay.

Unfortunately, it is common for responders who are unable to get a radio signal on their primary systems to be standing beneath a virtual rainbow of robust signals from other agencies, which they also are unable to access. My daughter has better technology in her cell phone than many public safety responders have in their voice and data systems.

Q. Major non-technology challenges?

A. For many agencies, outdated systems may be a symptom of a lack of maintenance and procurement planning and funding. When the Oregon SIEC set out to survey and inventory system owners (in order to establish a baseline picture of current and needed radio capabilities), it found that many small radio system owners cannot afford to employ their own technical staff. Instead, the owners rely heavily on contractors to operate and maintain their systems. This situation may generate a lack of awareness of short-term solutions—let alone long-term system needs.

Additionally, some system owners are aware of immediate and long-term needs, and look to interoperability grants for funding. Unfortunately, while many grants currently target "interoperability," in too many cases the grant money buys communication equipment that "could be" interoperable but actually is being used to just thicken the walls between the disparate communication silos.

Finally, while there are some fantastic exceptions, a tremendous lack of intergovernmental coordination and cooperation remains a formidable challenge. This lack of coordination and cooperation is not unique to government. Just take a look at how many different commercial cellular towers are on the same mountain top, when sharing a single tower would make more sense.

Q. Are there interoperability challenges unique to Oregon?

A. With a population of approximately 3.6 million, Oregon is the Nation's 27th most populous state. Yet, geographically, Oregon is the 9th largest state—spanning approximately 98,000 square miles. As a result, coverage and reliability vary significantly across the state.

Oregon's geography and topography create significant challenges for the state's emergency responders. The state is bisected—North to South—by two distinct mountain ranges. Additional mountain ranges crisscrossing the state create enormous signal shadows. As many know, providing a radio system in a flat state requires far fewer towers than does providing a system in mountainous terrain. We could save tremendous infrastructure money in Oregon if we could flatten the state's topography—an idea that has yet to catch on.

Oregon's four state agency radio systems also present a challenge. The radio systems are independently owned and operated. Due to a deferred approach to maintenance and upgrades, the public safety communications infrastructure of the State of Oregon is deteriorating, outmoded, and at severe risk of failure. Eighty percent of the state agency-owned towers and buildings need to be replaced, and radio equipment needs to be upgraded. In the technology and equipment arena, Oregon is coming to the starting line with considerably less than what many states already have in place.

Q. What is the Oregon SIEC's approach to these interoperability challenges?

A. The Oregon SIEC is different than other SIECs across the Nation in that it has a blended role. It advises and facilitates statewide intergovernmental planning, short-term interoperability solutions, and the conceptual design of a statewide public safety communications network. And, it addresses technology standards and frequency coordination. As one of its first efforts, in order to encourage coordination and modernization across agencies, the SIEC published the criteria for the state grant programs—specific to communications equipment and interoperability planning projects.

The Oregon SIEC champions a collaborative, local agency-involved approach. The structure of the Oregon SIEC was designed to include representatives from multiple public safety disciplines to ensure input and investment into the statewide strategy from all levels of government. In fact, approximately 50 percent of those who participate on the SIEC and its committees represent local government interests.

Q. What is the Oregon SIEC's vision for interoperable communications?

A. By statute, the Oregon SIEC is tasked with facilitating the development of the Oregon Wireless Interoperability Network. Intended to maximize shared use of a public asset, this single emergency response wireless communications infrastructure will support the public safety communications needs of all state agencies and ensure communications interoperability among all state, local, tribal, and Federal public safety agencies.

The SIEC envisions improving radio coverage to 85 percent statewide, with a minimum of 71 percent in each county—rather than focusing only on the most populated areas. Addressing radio coverage in each county—regardless of population—is important because there are emergencies in rural areas of the state that require a lone state trooper to call in backup, or require agencies to converge for a conflagration activation: forest fires in Oregon rarely occur downtown.

To ensure the success of the network, we are working with congressional and legislative delegates so that policy makers understand state and national interoperability needs. To this end, the Oregon SIEC supports the concept of creating a national forum for information sharing among SIECs nationwide in order to exchange lessons learned, and to encourage state-to-state interoperability planning and coordination.

2007 Technologies for Critical Incident Preparedness Conference and Exposition

The Departments of Justice, Homeland Security, and Defense will host the 9th Annual Technologies for Critical Incident Preparedness Conference and Exposition on November 6-8 in San Francisco, California. This event will highlight communications technologies and training tools available to emergency responders, and will engage stakeholders in order to identify requirements for tools under development. This year's conference is expected to draw 150 exhibits and 1,500 key emergency response leaders and decision makers. The event provides emergency responders, business and industry professionals, academic representatives, and local, tribal, state, and Federal policy makers with a forum to exchange ideas and collaboratively address critical incident technology and preparedness needs, protocols, and solutions. For the full conference agenda, or to register, visit www.ctc.org.

Denis Gusty to Lead Disaster Management Program

The Office for Interoperability and Compatibility's (OIC) Disaster Management (DM) program recently welcomed Denis Gusty, who will serve as DM Program Manager. Previously, Mr. Gusty led many of OIC's non-technical initiatives, including stakeholder coordination and statewide planning efforts.

Earlier this year, Mr. Gusty came 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 Information Technology policy and practices.

Interoperability TECHNOLOGY Today



Homeland
Security

A Resource for the Emergency Response Community

Summer edition 2007

"This edition features ..."

- Lessons learned from interoperability progress in Alaska
- A spotlight on Chief Jeff Johnson, SIEC Chair and President of the Western Fire Chiefs Association
- Success stories from the 2007 Industry Roundtable
- An overview of the 800 MHz rebanding process
- Broadband standards at a glance
- OPEN's successful field test at Super Bowl XLI

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

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