Summer 2006

Homeland Security

Interoperability·Today

A RESOURCE FOR THE EMERGENCY RESPONSE COMMUNITY

Interoperability No Gamble for Nevada

It was just after dawn in Las Vegas when a 911 call came in to the dispatch center reporting an accident involving a dump truck and a cargo tanker on the westbound lanes of the Tropicana Avenue Bridge over Interstate 15. The damaged tanker had sprayed cars and people with fine, oily droplets. Some of the drivers were leaving their vehicles and spreading contamination among bystanders. A motorcycle club traveling north on Interstate 15 had passed under the accident scene. As emergency responders reached the scene and assessed the situation, cell phone services became overloaded and unavailable. Other methods of communication had to be established as emergency response agencies from Clark County, the City of Las Vegas, and North Las Vegas worked together to bring the incident under control.

Fortunately for Las Vegas, this incident was a tabletop exercise, part of the Nevada Regional Communications Interoperability Pilot (RCIP) project. The February 21 exercise was the product of intensive planning by multiple jurisdictions and disciplines in the Clark County urban area, Nevada state agencies, and the SAFECOM program. Just two days later, a working group met to discuss and define actions to address the findings.

Tabletop exercises can help generate a strong learning process as well as help identify unutilized technologies and capabilities. The Las Vegas exercise made participating emergency responders aware of interoperability channels that were not being used to their full potential. The area's two mutual aid channels, International Calling Channel and International Tactical Channel, were functioning, but emergency responders had not been trained in their use or in standard operating procedures (SOPs) related to the channels. As a result, emergency responders were using cell phones and dispatchers instead of the channels. To address this issue, the tabletop exercise after-action report recommended collaborative training and adoption of SOPs by all agencies in the region.

"The biggest problem is just training the rank and file in use of the interoperability channels," says Louis Amell, chief of communications for the 911 call center that provides dispatch for all three jurisdictions. "Communications training often takes a back seat to other training that emergency responders and other emergency response professionals need to keep sharp at their jobs, due to a lack both of funding and of time. This exercise is prompting us to take a renewed focus on education and, from a dispatch center standpoint, to make sure that the people operating the radios know what is available to them."

In addition, and just as important, says Jim O'Brien of Clark County Emergency and Homeland Security Management, is the process used to develop the exercise. "Through working groups, through e-mails, and through planning, we really brought to the surface and reviewed ideas and concepts that had been long-held assumptions and found that they just didn't hold water," says O'Brien. "I think a lot of issues were resolved during the planning process."

Nevada is a somewhat unique state in that 70 percent of its population lives in the metropolitan Las Vegas area. The tabletop exercise helped strengthen alignment between state and urban area interoperability goals.

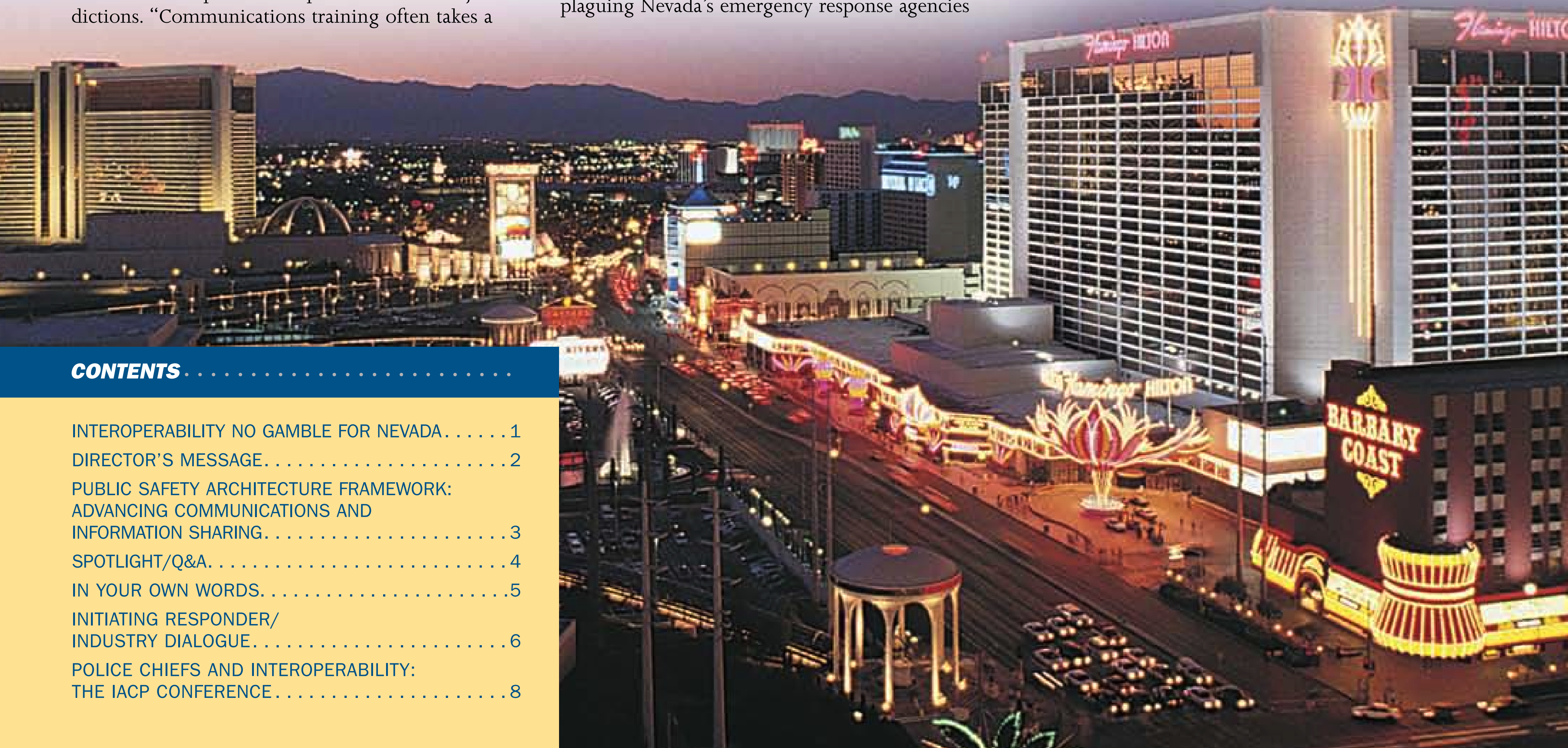
"We had a roomful of people, way more than I expected," O'Brien says, pointing out that the exercise involved not only law enforcement, fire services, and emergency medical services, but also hospitals, public health, public works, and government administration. "The diverse stakeholder involvement results in not just one agency making an argument to their funding source, because it's a collaborative effort that is documented through SAFECOM, a credible program."

SAFECOM's after-action report indicated that many of the problems that faced Nevada's emergency responders 15 years ago are the same problems plaguing Nevada's emergency response agencies today. Although there is greater awareness of the urgency of these issues, solutions still need to be developed to combat:

- Lack of awareness of existing assets
- Lack of procedures for using cross-agency, cross-disciplinary patches
- Lack of use of mutual aid channels
- Over-reliance on cell phones as workarounds

"Interoperability is a frustrating issue. We have the technology available to create a lot of interoperability, we just aren't using it well," Amell says. "The biggest thing is we need to make its use fairly routine."

The urban area project helped strengthen relationships between local and state emergency response stakeholders in the area and provided an opportunity for area leaders to resolve near-term issues. SAFECOM believes the momentum generated by this effort will help Clark County and Nevada maximize the use of existing capabilities for improved communications interoperability during incident response. SAFECOM intends to draw upon the lessons learned during the Nevada exercise as it develops future interoperability tools and models.



CONTENTS

About Interoperability • 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 to improve local, tribal, state, and Federal emergency response preparedness and response. Managed by the Science and Technology Directorate, OIC's mission is to facilitate the coordination of interoperability efforts across DHS. OIC, as a practitioner-driven office, is strengthening the ability of professionals' to work together to protect lives and property. SAFECOM, a communications program of OIC, works with its Federal partners to provide research, development, testing, evaluation, guidance, tools, and templates on communications-related issues to local, state, and Federal emergency response agencies.

Interoperability Today is published quarterly by the SAFECOM program at no cost to subscribers. Its mission is to provide the emergency responder community with information and updates regarding interoperability in emergency response communications, equipment, and training.

Subscriptions: *Interoperability 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 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 Today*, please notify us of any change in address or point of contact. Call toll free 866–969–SAFE (7233), or visit *www.safecomprogram.gov*, the 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 Today* may be reproduced. However, a statement of attribution, such as "This article was reproduced from the Summer 2006 edition of *Interoperability 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 Today* include Corbis, Fotosearch, Getty Images, and Veer.

UPCOMING

Events & Conferences

This listing provides information about upcoming events and conferences pertaining to interoperability.

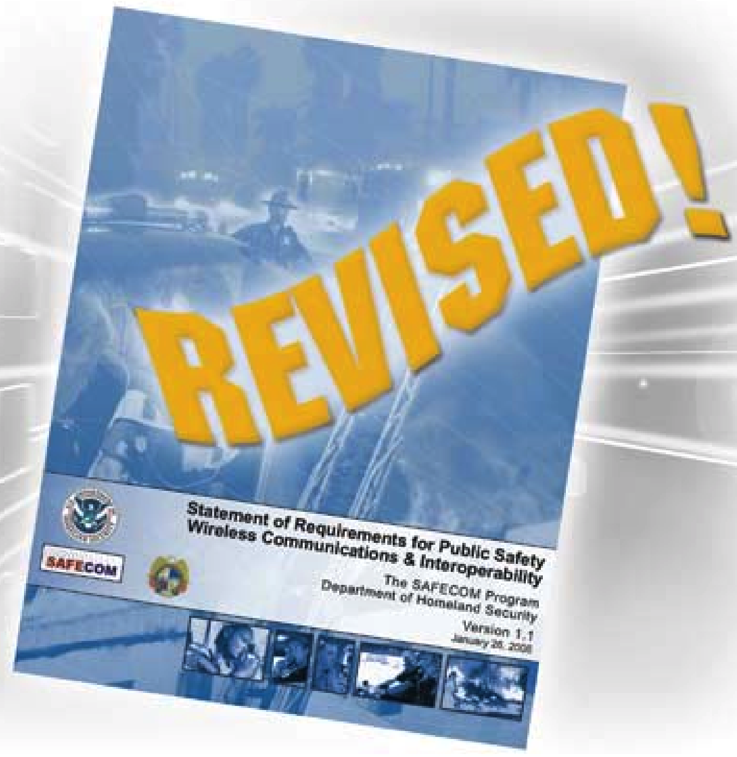
8th Annual Technologies for Critical Incident Preparedness Conference and Expo
September 6–8, 2006
Atlanta, Georgia
www.ctc.org

International Association of Fire Chiefs Fire-Rescue International 2006
September 14–16, 2006
Dallas, Texas
www.iafc.org

113th Annual International Association of Chiefs of Police Conference and Exposition
October 14–18, 2006
Boston, Massachusetts
www.theiacpconference.org

DIRECTOR'S MESSAGE

New Focus for Key Document


REVISED!
Statement of Requirements for Public Safety Wireless Communications & Interoperability
SAFECOM
The SAFECOM Program
Department of Homeland Security
Version 1.1
January 26, 2006

The *Statement of Requirements for Public Safety Wireless Communications & Interoperability* (SoR) was developed by SAFECOM in partnership with the National Institute of Justice's CommTech program and representatives of the emergency response community. This fall, SAFECOM plans to release a new version of SoR, version 2.0, which will begin to quantify the functional requirements for emergency response communications.

SoR version 2.0 will continue to focus on the communications and information-sharing requirements of emergency responders but will include new information on quantitative requirements. The current version of SoR emphasizes qualitative functional requirements for voice, data, image, video, and multimedia communications.

"Part of SAFECOM's overall technology approach is to identify technologies and interface standards necessary to achieve interoperability. That process starts by asking the users about their requirements," says Office for Interoperability and Compatibility Director Dr. David Boyd.

Qualitative vs. Quantitative

Versions 1.0 and 1.1 of SoR, released in April 2004 and April 2006, respectively, identified the qualitative parameters of communications and interoperability needs. Version 2.0 will begin to add a quantitative focus.

"We learned about their qualitative needs in the initial versions, so this new version will be a natural transition from capturing qualitative requirements first, then quantifying the quality of the services that emergency responders require," says Boyd.

To ensure SoR continues to accurately capture practitioner requirements, SAFECOM established an SoR Working Group, composed of representatives from law enforcement, fire services, and emergency medical services (EMS). This practitioner working group, created in early 2005, is responsible for vetting and upgrading SoR and evaluating any outside feedback or suggestions.

SoR version 1.0 presented practitioner requirements in multiple ways, including:

- Scenarios that present increasingly complex emergency responder situations, ranging from an ordinary police traffic stop to a car bomb explosion that involves response by multiple agencies
- Operational requirements broken out by discipline (i.e., law enforcement, fire services, and EMS)
- Functional requirements that describe qualitatively the applications and services needed, mobile devices features and functionality, and network performance

"Because the requirements are presented in different ways, the different sections may appeal to different audiences. For example, industry might focus more on the functional requirement sections because they build products and are interested in specific functional areas," Boyd says. "Emergency response professionals who are interested in how the requirements affect them may prefer to focus on scenarios to which they can relate."

Assistance Needed

As SAFECOM further develops SoR, the program continues to seek practitioners who want to participate in the development process.

"We're particularly interested in finding practitioners who have real-world experience, because they have an understanding of and real experience with what's required," Boyd says. "Finding an adequate number of practitioners to support lab testing (which helps capture user requirements) is one of the challenges we face."

Congratulations to Dr. Boyd!

The U.S. Department of Homeland Security recently honored Dr. David G. Boyd, a recipient of the 2005 Presidential Rank Award for Meritorious Executive. This prestigious award recognizes outstanding career members of the Senior Executive Service who have consistently demonstrated strength, integrity, industry, and a steadfast commitment to public service. Through his leadership of the Office for Interoperability and Compatibility, Dr. Boyd drove progress in interoperable communications by developing tools and resources to help the Nation's emergency responders strengthen emergency preparedness and response.

Public Safety Architecture Framework: Advancing Communications and Information Sharing

SAFECOM developed the Public Safety Architecture Framework (PSAF) to advance the program's goal of making communications and information sharing interoperable among emergency response organizations. SAFECOM's *Statement of Requirements for Public Safety Wireless Communications and Interoperability* (SoR) outlined the program's vision of interoperable communications. The PSAF, in turn, provides an industry-validated methodology that emergency response agencies can use to make the transition from "as-is" systems to the desired "future state"—truly interoperable communications.

Emergency responder agencies seeking to identify gaps in interoperability and technologies to bridge these gaps will find PSAF an effective tool. The PSAF framework is a methodology that will give emergency response agencies a "common language." Agencies can use this common language to pinpoint specific areas in their communications systems that are not interoperable and to identify what they need to do to address those gaps. PSAF will also give agencies a common language for communicating with the technicians and suppliers tasked with addressing interoperability in emergency response wireless communications networks.

The PSAF is being developed in three volumes. The first two volumes are directed to enterprise architects and engineers. Volume I provides definitions, guidelines, and background material. Volume II contains more detail on PSAF's three architectural perspectives, or "views," of emergency response communications and information systems:

- **Operational View:** Used to model the emergency response agency's communication flows
- **Systems View:** Used to model the systems that support the communication flows
- **Technical Standards View:** Used to model the standards that comprise the systems that support the communication flows

Together, these three architectural views and the data elements they contain comprehensively describe the architecture of a communications or information system. Volume II also provides information on the products, or "model descriptions," available to support the three views. *PSAF Volume I* and *PSAF Volume II* are available on the SAFECOM Web site for downloading and review (see sidebar).

A third volume, which will be a user's guide, is still under development. *PSAF Volume III* will document procedures for using the methodology outlined in volumes I and II as well as a supporting software tool.

This Web-based software, which will be vetted by the practitioner community, is central to PSAF. With this tool, emergency response agencies will be able to model their communications systems with common terms, so that they can then compare their systems for how interoperable they are. Using a common data model, the software will facilitate creation of the architectural views of each individual communications system. The software will compare and analyze these views to highlight where the systems are interoperable and where they are not. With this information, the agencies can develop a plan to make their respective systems more interoperable. Agencies can also use the software tool as a planning aid for equipment updates and upgrades.

The designers of PSAF envision four primary uses for the tool:

- Providing a process and tools that emergency response agencies can use to plan for interoperability and information sharing
- Helping to identify areas in current and future systems that are not interoperable
- Protecting current communications systems during the transition to the future systems that meet SoR requirements
- Making products more efficient by leveraging commercially available equipment that meets required standards

The ability to go to a supplier and ask for equipment that meets specific standards will empower emergency response agencies to get the equipment they need to be prepared to respond to an emergency. With input from the field, PSAF will evolve to include lessons learned from actual users and will become a comprehensive guide that supports the efforts of local, tribal, state, and Federal agencies working together to protect the public.

Volumes I and II of the Public Safety Architecture Framework are available on the SAFECOM Web site.

- ***Volume I: Definitions and Guidelines*** **can be downloaded at:** *www.safecomprogram.gov/SAFECOM/library/technology/1251_publicsafety.htm.*
- ***Volume II: Product Descriptions*** **can be downloaded at:** *www.safecomprogram.gov/SAFECOM/library/technology/1252_publicsafety.htm.*

These documents are technical guides for use by communications professionals knowledgeable about interoperability issues.

SPOTLIGHT

Raymond Hayling: Taking the Lead for Interoperability in New Jersey

In December 2004, Raymond J. Hayling II was appointed to serve as New Jersey's first chief public safety communications officer, a position within the Office of the Attorney General. In the interest of unified law enforcement, New Jersey designates its attorney general to be the state's chief law enforcement agent. As such, the attorney general oversees the New Jersey State Police and the Division of Criminal Justice. As the man in charge of improving interoperable communications, Chief Hayling shares responsibility for law enforcement and works regularly with state troopers, county sheriff's departments, and municipal police officers.

Judging from his education, few could have imagined Hayling's current occupation. Hayling attended Seton Hall Preparatory School, the oldest Catholic preparatory school in New Jersey, and graduated from Rutgers University in New Brunswick, where he received a degree in chemical engineering. "Beyond mathematics and applied science, what I learned at these institutions was to be a critical thinker and a self-starter," says Hayling.

Early in his career, Hayling worked for Fighting Back, a national program of the Robert Wood Johnson Foundation that supports community initiatives to reduce substance abuse. While working there, Hayling held several positions directly or indirectly connected with management information systems. These jobs required Hayling to travel to urban areas nationwide. "I think working for this nonprofit organization prepared me well for my current position," he says. "There I developed the ability to listen, learned to take a scientific approach to nonscientific issues, and realized that you need to get out and see a problem first hand."

Hayling later worked for the New Jersey Institute of Technology, where he held several senior management positions involving communications, technology, and Internet services. Hayling was working at the institute when the 1995 Oklahoma City bombing occurred. The deficiencies of the rescue underscored for Hayling the importance of effective communications to emergency responders' mission-critical duties. "I heard the stories of runners having to pass information from commander to commander and of the inability of law enforcement, fire, and emergency medical services personnel to coordinate effectively the search and rescue mission after that horrific incident."

Hayling's concern about interoperability intensified in the aftermath of September 11, 2001. "As a person who believes in using technology as a tool, I realized that the inability of emergency responders to communicate could cost their lives and the lives of others as well."

Hayling carried this deep interest in interoperable communications with him when he went to work for the State of New Jersey—first as assistant chief of operations and management for the Office of the Governor, and later as chief of staff for the Office of Information Technology and executive director of the Office of the Attorney General. Since serving as New Jersey's chief public safety communications officer, says Hayling, "The key challenges that have been overcome were improving interagency cooperation, getting people to realize that a lack of interoperability is a symptom of poor communications planning, and getting people to see that there is no silver bullet for dealing with interoperability issues."

Several of Hayling's interoperability initiatives are grounds for pride. "The New Jersey Interoperability Communications System is one of the initiatives that I am most proud of. The system is a series of region-specific interoperable communications assets. These assets include a statewide radio cache of more than 2,000 radios, 21 interconnect switches, 17 tactical interoperability channels, and at least 2 regionwide interoperability channels per region. We are also in the process of developing a Statewide Interoperability Communications Task Force composed of a team of communications specialists for each region of New Jersey. The teams will train together and assume the roles of communications unit leaders during incidents.

"Interoperable communications are invaluable to New Jersey and the Nation," Hayling continues. "In any incident, large or small, poor command and control spells trouble. Without interoperable communications, effective command and control doesn't exist. Lack of interoperable communications can also turn what otherwise would be an effective response into a painfully slow response or an uncoordinated mess due to a lack of timely information."

Q&A with Raymond J. Hayling II

Chief Hayling was born in Los Angeles, California. During his primary school years, his family moved to New Jersey. He currently resides in Somerset County.

Q. What made you interested in seeking your current job?

A. I saw the position of chief public safety communications officer as an opportunity to help resolve many of the communications issues made more apparent by the September 2001 attacks and to make a difference in public safety in my state.

Q. What has been New Jersey's biggest hurdle in interoperable communications so far?

A. It is difficult to single out one hurdle because they are all tied together. The biggest hurdles have been dealing with a government bureaucracy that does not understand public safety communications, poor cross-jurisdictional communications planning, home rule (each jurisdiction wanting to do everything itself and tending to resist state coordination), lack of funding, and obtaining the radio frequencies needed for public safety communications.

Q. In your view, what are the best interoperability solutions for New Jersey or any state?

A. There is no one solution. Varied and flexible interoperable assets that allow emergency responders to adapt to the emergency and disaster situations are best. Having both mobile and fixed infrastructure is also very important.

Q. What interoperability initiative is your priority now?

A. Right now, we are in the process of putting together regional communications systems. We are looking for funding and technology that will allow multiple agencies across a region to communicate in a more seamless manner.

We want to alleviate the financial burden on all of the agencies now maintaining separate communications infrastructures. Solving this funding problem will simultaneously give us the opportunity to plan interoperability into the design of new systems.

This approach will have the added benefit of simplifying the communications landscape. The state currently has more than 2,000 radio systems. If we can reduce the number to about 30, the logistics involved in planning better communications becomes much less daunting. The thought is that if we can more efficiently utilize the assets we already have in place, the state will be in a better position to provide for growth and make improvements when we get the additional 700-MHz frequencies.

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

A. I think that I would be working on the diplomatic end to keep the United States and its allies safe from terrorists and rogue states. Communications is much more than a technological issue, although the technology does tend to get the most attention.

The State Department would be a good place to work, but I see business as fertile ground for diplomacy too. As the global economy grows, businessmen serve as spokesmen for their home countries. In the course of bringing opportunity to parts of the world that have little or none, American representatives of business can help change people's views of the United States and our way of life.

IN YOUR OWN WORDS

Breaking the Emergency Management Information Barrier

By Chip Hines, Acting Director, Office for Interoperability and Compatibility

Imagine you are unable to send an e-mail to a friend because the e-mail software system is incompatible with your software system. Thankfully, this isn't a problem with e-mail, but for emergency responders, incompatible communications systems are an everyday challenge.

Fast, accurate delivery and exchange of data during a disaster saves lives. Unfortunately, disparate software systems unable to "talk" to each other often prevent emergency responders from sharing vital information needed to perform their mission-critical duties. Often they will have to rely on time-consuming telephone calls to ensure that the information gets through.

We have made great strides in interoperable communications technologies, but there remains much to be done. As information technology improves, software products often become more proprietary, multiplying the disconnect between the disparate systems. To rectify this problem, there is an immediate need to develop messaging standards for transferring critical data over software and communications platforms. Thanks to the partnership efforts of the emergency response community, government, and industry, the groundwork for messaging standards development is underway.

The Office for Interoperability and Compatibility's Disaster Management (DM) program is assisting emergency responders and industry with standards development efforts through its Messaging Standards Initiative. This initiative aims to leverage existing relationships and technology to create uniform data-sharing mechanisms and standards. The standards will enable emergency responders to share critical information before, during, and after an emergency.

The initiative's partnership approach to developing standards has several advantages:

- Ensures practitioners' requirements are heard and are technologically feasible.
- Allows industry to focus on adding value to final products' capabilities and ease of use by sparing industry from determining what information needs to be exchanged.
- Encourages the implementation of adopted standards into final products.

Moreover, this approach makes certain that the standards development process is practitioner driven rather than technology driven by:

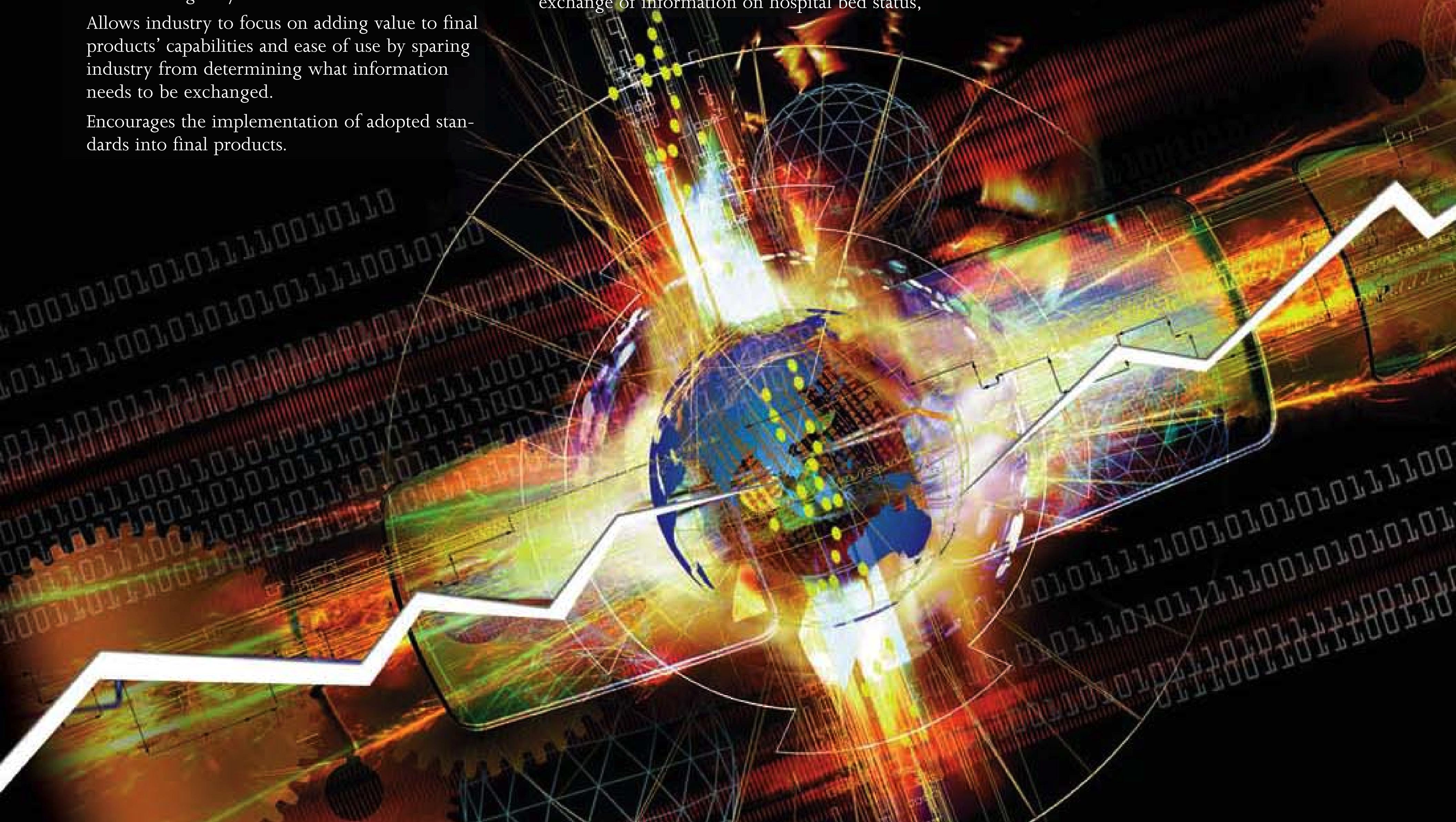
- Promoting a more responsive and effective vendor community, which results in more choices for emergency responders.
- Ensuring emergency responder participation in the standards development process.
- Leveraging existing technical work, especially in terms of common data standards.
- Allowing users to choose software that best meets their needs and enables them to seamlessly exchange information with other industry products.

The widespread use of the Common Alerting Protocol (CAP) 1.1 is a testament to the success of this approach to standards development. CAP, approved in October 2005, is a standard alerting message that can be transmitted across software and hardware systems daily. The standards below reinforce the value of a practitioner-driven development process.

- **Distribution Element (DE) Messaging Standard:** This standard enables emergency responders to distribute information to specific recipients—police, fire, and emergency medical services—designated by geographic area or agency code. The DE draft standard was submitted to the Organization for the Advancement of Structured Information Standards (OASIS) and became an international standard on May 1, 2006.
- **Resource Messaging (RM) Standard:** RM is a suite of 17 standards that enable an emergency responder to request a specific tool or resource such as a vehicle or specialized personnel. RM standards also include response and resource management capabilities. The draft RM standards suite was submitted to OASIS in October 2005.
- **Hospital Availability Exchange (HAVE) Standard:** This standard will facilitate the exchange of information on hospital bed status, capacity, and resource availability between medical and health organizations and emergency information systems. HAVE will enable on-scene emergency responders to move victims to the facility best equipped to handle additional patients. The draft HAVE standard was submitted to OASIS in January 2006. The emergency response community is also using a Department of Justice (DOJ)-sponsored initiative known as the Global Justice Extensible Markup Language (XML) Data Model (Global JXDM). Global JXDM includes a data model, a data dictionary, and an XML schema.

Global JXDM is the base technology for the National Information Exchange Model (NIEM), which is cosponsored by DOJ and the U.S. Department of Homeland Security (DHS). Through NIEM, DOJ and DHS aim to provide the groundwork for national interoperable information sharing and data exchange. NIEM has involved the collabor ative work of DM representatives, the global initiative, and other local, tribal, state, and Federal agencies.

Though the development, approval, and implementation of these standards is a monumental task, it only marks the beginning of the DM's standards-related initiatives. Additional standards are needed for information sharing to be truly effective during both emergencies and day-to-day activities. Practitioner awareness of and participation in the Messaging Standards Initiative is central to the effort's capacity to deliver timely and effective results for improving communications interoperability. To that end, I hope you will join me in calling for the rapid development and use of standards for information exchange in emergency management. Tell the vendor community that you expect it and will only purchase products that comply with these standards. Together we can establish a community that is truly able to exchange incident-related information without regard to the specific software in use.



Initiating Responder/Industry Dialogue

This article highlights the inaugural SAFECOM Industry Summit and the importance of dialogue between emergency responders and industry in pushing progress in interoperable communications.

> ***"The interoperability problem is 90 percent coordination, 10 percent technology"***
>
> *—Chris Essid*
> *Commonwealth Interoperability Coordinator*
> *Commonwealth of Virginia*

Strong, continuous dialogue and cooperation between the emergency response community, government, and industry are critical success factors for strengthening interoperable communications.

That was a key message of SAFECOM's inaugural Industry Summit, which provided a forum for SAFECOM to update members of industry on its progress and programs and for emergency response representatives to engage with industry on key interoperability issues.

Speakers at the conference, held in March 2006 in Washington, D.C., emphasized the need for increased coordination between different emergency response disciplines, between levels of government, and between the emergency response community and industry. The consensus was that the more engaged these groups are, the more successful interoperability initiatives will be.

"The interoperability problem is 90 percent coordination, 10 percent technology," is the message Chris Essid, Commonwealth Interoperability Coordinator, Commonwealth of Virginia, gave the gathering. "Forums like this are outstanding to help solve this problem."

Capt. Eddie Reyes of the Alexandria (Virginia) Police Department said the conference provided a good opportunity for emergency responders to meet with the vendor community and discuss standards and training in communications. "This is about coming out and meeting the vendors face to face," he said.

The emergency response community ideally expects a level of interoperability that is transparent to the user—a standards-based, practitioner-driven system or approach that allows emergency responders to communicate data and voice on demand across jurisdictions and across disciplines with their own equipment and with limited effort.

Primary technology concerns voiced by emergency response representatives included:

- **Backward compatibility.** New radio technology needs to remain compatible with legacy systems so that when a jurisdiction upgrades its system to another version, it will not lose existing compatibility with its neighbors.
- **Ease of use.** Manuals for equipment are often lengthy and complicated. Manufacturers need to simplify directions to help users become familiar with the equipment.
- **Training.** Users need adequate training to understand the complexities of the equipment.
- **Redundancy.** Systems must have duplicate backup components that would take over should a system fail.
- **Reliability and resilience.** Communications equipment and networks must be able to operate in natural or manmade disasters and work in environments involving chemical, biological, radiological, nuclear, or explosive materials.
- **Compatibility.** Equipment from one manufacturer should be functionally compatible with equipment from other manufacturers.
- **Open systems.** Emphasis should be on open architecture rather than proprietary systems.

"The focus of this conference is to help industry understand this practitioner-driven initiative—that we are trying to look at a 'system of systems' approach, that we are looking for open architecture, not a proprietary standards kind of approach," says Dr. David Boyd, Director, Office for Interoperability and Compatibility, U.S. Department of Homeland Security (DHS).

continued on page 7

INDUSTRY SUMMIT • *continued from page 6*

According to Boyd, local, tribal, state, and Federal agencies face a host of challenges and competing needs, and interoperable communications is only one of the issues.

Funding for interoperability communications has grown in recent years. Between fiscal years 2003 and 2006, Federal agencies provided approximately $2.1 billion in grants to states and localities for interoperability projects, Boyd says. For fiscal year 2007, states will be required to develop an interoperable communications strategy as a condition for receiving DHS grants.

During the conference, speakers also addressed the *Statement of Requirements for Public Safety Wireless Communications & Interoperability* (SoR), standards development, and conformity assessment.

Stating Requirements

SoR version 1.0, released in 2004, is a practitioner-driven set of communications requirements. It defines communications requirements for voice and data communications in day-to-day, task force, and mutual aid operations.

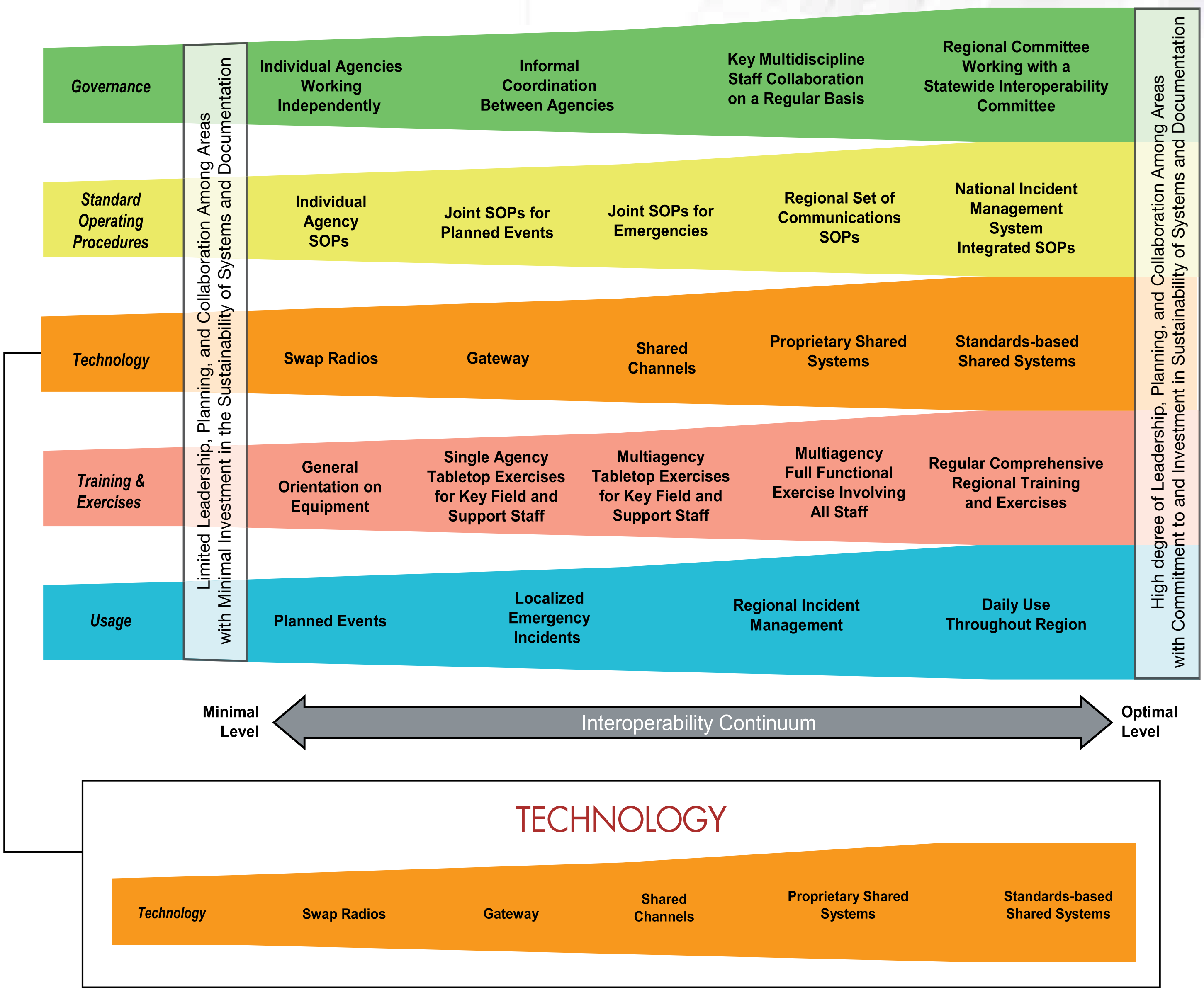
"The SoR is the first time there has been an attempt in a single document to pull together the capabilities and requirements emergency response practitioners say they need to achieve interoperability," Boyd says. "The SoR is a device that the emergency response community can use for building their business cases for systems. It's a tool that can be used by industry to figure out what they need to build to."

Setting Standards

Achieving the emergency response community's desired level of interoperability requires standards to define how components of emergency response communications systems will function compatibly, regardless of manufacturer. Standards allow agencies to procure equipment from multiple sources and provide ease of use. Standards also help industry by making technology decisions less risky for manufacturers.

An example of this standards-based approached can be seen in Project 25 (P25), a user-driven standards effort supported by major land mobile radio (LMR) manufacturers and Federal, state, and local emergency response organizations. P25 is a suite of emergency response radio communications standards dedicated to ensuring that digital radios from different manufacturers can communicate in emergency situations. P25 includes eight interfaces, the standards for which are in various stages of completion or development. Each interface allows the products of one manufacturer to communicate with products of other manufacturers by defining the signaling and messages that cross the interface.

Interoperability Continuum


Governance
Individual Agencies Working Independently
Informal Coordination Between Agencies
Key Multidiscipline Staff Collaboration on a Regular Basis
Regional Committee Working with a Statewide Interoperability Committee
Standard Operating Procedures
Individual Agency SOPs
Joint SOPs for Planned Events
Joint SOPs for Emergencies
Regional Set of Communications SOPs
National Incident Management System Integrated SOPs
Technology
Swap Radios
Gateway
Shared Channels
Proprietary Shared Systems
Standards-based Shared Systems
Training & Exercises
General Orientation on Equipment
Single Agency Tabletop Exercises for Key Field and Support Staff
Multiagency Tabletop Exercises for Key Field and Support Staff
Multiagency Full Functional Exercise Involving All Staff
Regular Comprehensive Regional Training and Exercises
Usage
Planned Events
Localized Emergency Incidents
Regional Incident Management
Daily Use Throughout Region
Limited Leadership, Planning, and Collaboration Among Areas with Minimal Investment in the Sustainability of Systems and Documentation
High degree of Leadership, Planning, and Collaboration Among Areas with Commitment to and Investment in Sustainability of Systems and Documentation
Minimal Level
Interoperability Continuum
Optimal Level
TECHNOLOGY
Technology
Swap Radios
Gateway
Shared Channels
Proprietary Shared Systems
Standards-based Shared Systems

Assessing Compliance

Compliance assessment is a way to demonstrate conformity to standards in product development. Compliance testing can serve to catch equipment defects early and reduce costs to both industry and emergency response customers. The risks associated with noncompliance include an overdesigned system, which could increase cost, and an underdesigned system, which could lead to loss of confidence in the system.

The National Institute of Standards and Technology (NIST), with the support of SAFECOM and the P25 steering committee, is developing a P25 Compliance Assessment Program. The primary objectives of the program are to assure users that a product is interoperable and to identify equipment problems before equipment is used in the field. The program will include third-party testing by NIST-accredited independent laboratories.

Manufacturer participation in the program would be voluntary. Manufacturers would own and control release of test reports and can sell products at any time irrespective of participation in the program. Preliminary implementation of the program is expected to begin at the end of 2006.

Police Chiefs and Interoperability: The IACP Conference

This October 14–18, more than 16,000 emergency response community representatives are expected to convene in Boston, Massachusetts, for the 113th Annual International Association of Chiefs of Police (IACP) Conference and Exposition. The Law Enforcement Education and Technology Exposition will feature seminars, workshops, and forums. Members of IACP's committees will lead many of these sessions.

IACP is the oldest and largest nonprofit law enforcement association in the world. With 20,000 members representing 89 countries, IACP is the Nation's only law enforcement group that includes chiefs from state and local agencies and jurisdictions of all sizes. The association's goals include developing and promoting scientific and technological advances in law enforcement.

A strategic plan helps guide IACP's internal operations. To ensure that the association's goals are aligned with relevant issues in law enforcement, a strategic planning committee reviews and updates this plan regularly. The current plan focuses on several topics, including education about and acquisition of new technology. So that this part of the plan is successfully adopted, IACP is devoting much of its energies and resources to technological pursuits.

IACP is organized into divisions, committees, and sections that each address specific law enforcement issues. IACP's Criminal Justice Information System Committee works with the Federal Bureau of Investigation to gather and publish crime statistics. IACP's largest section, the Law Enforcement Information Management Section, oversees computer and records management. The Law Enforcement Information Technology Standards Council is developing universal standards for strategic planning and implementation of technology in law enforcement. IACP's "one-stop shop" for technology-related information, the Technology Clearinghouse, received more than two million Web site hits last year.

The IACP Communications and Technology Committee, composed of 30 IACP members, is one of the most active committees within IACP. The committee focuses primarily on wireless communications issues, both technical and operational, for law enforcement. The committee ranks interoperability as one of its top agenda items. The committee has been deeply involved with addressing issues of radio spectrum, funding for communications systems, 800-MHz rebanding, narrowbanding of emergency response systems below 512 MHz, issues relative to rules, and other issues regarding the new emergency response spectrum in the 700-MHz band at 4.9-GHz band. The chair of the committee serves as the IACP representative on the U.S. Department of Homeland Security's SAFECOM Executive Committee and also serves as the IACP representative to the National Public Safety Telecommunications Council (NPSTC). The IACP has been a strong supporter of the SAFECOM program and has contributed input from the law enforcement community during the development of various SAFECOM documents.

Because ongoing research is critical to developing new law enforcement techniques and technologies, the association established the IACP Research Center. The center partners with other national organizations and the Federal government—primarily the U.S. Department of Justice—to conduct research and publish findings on issues of significance to law enforcement. The center researches issues that affect the workings of both large and small law enforcement agencies, including technology, officer safety, violence against women, mentoring, and technical assistance. To complement its research findings, the center offers training to more than 3,000 law enforcement officers each year and provides technical assistance to individual agencies by request.

In addition to research, IACP publishes a monthly magazine, *The Police Chief,* with a circulation of more than 21,000. The magazine is a comprehensive source that reports the latest information on policies, training, and best practices. The publication also provides professional guidance in areas ranging from current law enforcement issues to challenges faced in the field.

For members of law enforcement agencies, a command- or administrative-level position is a criterion for active membership in IACP. However, the association's membership extends beyond police chiefs to include individuals affiliated with law enforcement in a wide range of professions, from city managers to brigadier generals to doctors and handwriting examiners.

For more information:

- IACP: *www.theiacp.org*
- The Law Enforcement Information Technology Standards Council: *www.leitsc.org*
- *The Police Chief* magazine: *www.policechiefmagazine.org*
- IACP Technology Clearinghouse: *www.iacptechnology.org*
- The Research Center at IACP: *www.theiacp.org/research/*
- The IACP Annual Conference: *www.theiacpconference.org/*

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

Interoperability • Today
A RESOURCE FOR THE PUBLIC SAFETY COMMUNITY