Solutions for Communications

Voice and Data Interoperability

This issue of TechBeat features developments in voice and data communications technology and how they are promoting public safety information sharing and interoperability.

Interoperable voice and data communications are critical to effective coordination among public safety agencies. Information-led policing involving data sharing and analysis can lead to more effective law enforcement.

Efforts to solve interoperability challenges in the public safety community include creation of the Global Justice Information Sharing Initiative (Global), which advises the U.S. Department of Justice on justice information sharing and integration initiatives. The Global Justice XML Data Model (Global JXDM) is a standard designed specifically for criminal justice information exchanges. Global JXDM removes the burden from agencies to independently create exchange standards.

As technologies emerge, communications options improve. Highlighted here are a few of the recent efforts to enhance, ease, and expedite public safety communications.

Talking in Texas With TIP

When a tornado hit the area around Eagle Pass, Texas, in the spring of 2007, local police were able to readily communicate with other Texas emergency responders who offered assistance, thanks to a regional communications improvement project known as TIP.

TIP, the Technology Improvement Project for the Middle Rio Grande Region of Texas, is a Project 25 (P25)-compliant, spectrum-efficient, VHF-trunked infrastructure system that is shared with local, State, Federal, and tribal users. The area served by the system covers roughly 15,000 square miles in 9 counties, with a population of 155,000. P25 is a suite of standards intended to help produce equipment that is interoperable and compatible regardless of manufacturer.

“People came in [from the other counties] and we were able to communicate,” says Sgt. Alejandro Guedea of the Eagle Pass Police Department. “You could pick up a radio, switch to the frequency, and could all communicate together, as opposed to contacting your dispatcher, who would have to communicate with another dispatcher.”

Although no 700/800 MHz users are currently assigned to the region, the system design includes the capability to communicate with users in those bands who might be called on to assist during an emergency.

“The system gets everybody on the same page,” says W. Spade Condy, telecommunications coordinator for the Middle Rio Grande Development Council (MRGDC), which is directing the project. “Using trunking allows us to take advantage of the towers, to fill in some of the [communication] gaps and holes in radio coverage we had previously encountered. We set up radio common programming templates when we first started, and set up zones that are named consistently across the entire region. The equipment is also backward compatible and will operate on legacy systems as well as new ones.”

(See Talking in Texas With TIP, page 3)

Share a Photo, Catch a Criminal

Approaching the driver of a car stopped for running a red light, the officer asks for identification. After checking all of his pockets, the driver says he must have left his wallet at home and proceeds to rattle off a name and an address in another State. In the past, the officer might have let the driver go with a warning or a citation for not carrying his license. Thanks to a new program facilitated by Nlets (the International Justice and Public Safety Network), the officer requests not only the driver’s information, but also his photo, from the neighboring State, and receives it directly in his patrol car.

Confronted with a photo that obviously is someone else, the driver breaks down and admits he gave a friend’s name and address to avoid the officer’s finding out about his past criminal record.

(See Share a Photo, page 2)
During 2007 and 2008, Nets applied grant funding received from the Office of Justice Programs’ National Institute of Justice (NIJ) in an effort to take the lead on a pilot project that permits the exchange of departments of motor vehicle (DMV) driver’s license images. The project deploys a limited operational capability to allow States to exchange electronic DMV images solely for the purpose of positive identification.

Phase I of the project went online in March 2008 when Oregon and North Carolina became the first two States to exchange photos. Since then, Nets has immediately begun implementing the next phases of the program, which involve bringing other States online and establishing the exchange of other types of photos, such as inmate images and booking photos.

“Everything is going great. There are no performance issues at all,” says Bonnie Locke, Nets director of program management. “One thing we plan to do in the next phase is make sure that States that want to participate but aren’t yet in a position to send photos out are able to receive them. This will still provide a huge benefit to States that aren’t quite ready, financially or for other reasons, to send their photos out.”

“This is a number one priority with law enforcement around the country,” says George Ake of the Border Research and Technology Center (BRTC) in Austin, Texas, which has provided support to Nets on this project. “Being able to obtain driver’s license photos is a huge concern in the field because officers want to know who they are really talking to. A lot of times officers have to let people go who need to be detained because they have no way of knowing their true identities. With this system in place, they can have the photo at their patrol car in a matter of seconds.”

BRTC is part of the National Law Enforcement and Corrections Technology Center System, which is a program of NIJ.

Some of the situations in which the availability of a driver’s license photo could prove useful include the following:

- Confirming whether an individual is who he or she claims to be.
- Revealing instances of possible identity theft.
- Identifying a specific person sought in connection with a criminal activity.
- Making it more difficult to obtain access to photos (for example, some States require a written request on letterhead), law enforcement agencies will be able to say to the legislature that they are benefiting from getting photos from other States, and there would be even more benefits if they could also send photos out. We hope to build on this and spread it across the country over the next few years,” Locke says.

There are also States that need to upgrade their technology, while others simply do not realize they already have the necessary technology and policies in place. Nets is working to ensure that every State receives a presentation about the project.

For more information on Nets, visit www.nlets.org for specific information on the project, contact Bonnie Locke at blocke@nlets.org.

Nets has drafted model policy documents and procedures. Each State has its own rules, issues, and laws. Nets does not attempt to dictate to them but merely offers a model, Locke says.

“What I hope will happen is that in States where it is more difficult to obtain access to photos (for example, some States require a written request on letterhead), law enforcement agencies will be able to say to the legislature that they are benefiting from getting photos from other States, and there would be even more benefits if they could also send photos out. We hope to build on this and spread it across the country over the next few years,” Locke says.

What Is Nlets

The International Justice and Public Safety Network, or Nets, has been in the business of connecting law enforcement and the justice community for nearly 40 years. Today, Nets is a state-of-the-art secure sharing system dedicated to the entire justice community. Its sole purpose is to provide for the international, interstate, and interagency exchange of criminal justice information. It uses leading-edge technology such as Web services and service-oriented architecture to serve its customers.

Nets is a nonprofit corporation chartered by the States and funded by user fees. The members are all 50 States, the territories, all Federal agencies with a justice component, and the Royal Canadian Mounted Police.
The multiagency project covers nine counties in the Southwest border region of Texas—Dimmit, Edwards, Kinney, LaSalle, Maverick, Real, Uvalde, Val Verde, and Zavala. Val Verde and Maverick training, which are along the Rio Grande River border with Mexico, were the first to become part of the system in 2002. Other counties followed. Real and Edwards counties will probably be the last to become fully operational. All nine counties are anticipated to have some trunk system capability operational by the fall of 2008, with full functionality for all counties expected in early 2009, according to Forrest Anderson, MRGDC homeland security director. Other agencies in Texas have also expressed interest in the system, and planners anticipate adding jurisdictions beyond the original nine counties.

MRGDC is a regional government organization providing multiple services to the area. MRGDC plans and delivers economic development efforts, helping to get federal funds to support local projects. Its varied services also include management of the region’s 911 emergency response system, funding for the Regional Law Enforcement Training Academy to train local peace officers, basic education and skills training services for the unemployed, and a network of service centers for the elderly.

The Border Research and Technology Center (BRTC) in Austin, Texas, operated by the Sheriffs’ Association of Texas, has been providing technology assistance for TIP. BRTC is part of the National Law Enforcement and Corrections Technology Center System, a program of the Office of Justice Programs’ National Institute of Justice (NIJ). Federal funding for TIP has been channeled through NIJ.

TIP replaces communications systems purchased with law enforcement assistance grant funds 30 years ago. Coverage in many cases is poor in some areas and at best unreliable in others with the old single-county, single-agency radio systems.

"Under the old system, each county had a radio tower in the county exclusive to that county," explains Joe Peters, BRTC director. "If users went outside the range of that tower they didn’t talk to anyone. With the new trunk system, the towers complement each other; users never know which tower they are talking on."

The system provides individual talk groups for each user agency and talk groups dedicated to local and regionwide interoperability.

"Another useful feature is they can roam across the entire region," Peters adds. "If a deputy sheriff in Val Verde had to go to La Salle County, he can still keep up with what is going on in Val Verde. All the radios are programmed alike. If during a mutual aid incident a responder picks up a radio in another county, the radio will work exactly as his does. The nomenclature is the same throughout the region. There are interoperability channels throughout the region, and private talk groups so that a sheriff does not have to listen to the fire department if he doesn’t want to, but he has the capability to do so."

"It takes a lot of the effort out of using the equipment during a stressful incident," Condry says. "You just dial in to a talk group and can talk to them. You can also tie into other systems, so for interoperability it works very nicely."

The best radio for interoperability is the radio that the public safety providers use every day.

"Life for the first responder community in the region served by the TIP project would be like a step back in time without it," Peters says. Users of the new system now enjoy a heightened sense of security and comfort in knowing that when they ‘push to talk’ on the new system, someone, somewhere, is likely to hear them from almost anywhere across the almost 15,000 square miles served by the system. They now enjoy being able to utilize the latest in technology to enable much improved coverage and seamless interoperability between the local, tribal, State, and Federal users of the system with the radios they are most familiar with, the radios they use in their everyday operations."

A number of the agencies served by the system are small and rural. Using the VHF band allows more radio coverage in a rural area. With VHF, Anderson explains, they can cover 5,000 square miles using 15 VHF trunked radio repeater sites. An 800 MHz system could require roughly double the number of sites at considerably greater expense for the same amount of coverage across the region.

"It’s cost efficient and spectrum efficient," Anderson says.

Estimated cost for the project upon completion is about $8 million. Initial funding was used to improve infrastructure—the equipment at the towers, which had to be in place first. Other dollars are used for purchase of mobile and portable radios and a regional records management system to facilitate data sharing among the law enforcement agencies across the entire region. Jurisdictions are also using grants from the U.S. Department of Homeland Security to equip their fleets with subscriber radios.

The Eagle Pass Police Department has been buying new subscriber equipment as it receives grants, and expects to have all officers and vehicles outfitted with the updated radio equipment by fall 2008. "Our officers are looking forward to it as a safety issue," Gueda says.

The TIP project required extensive frequency and propagation studies to determine the best locations to install communications equipment. Legacy tower sites were chosen to maximize radio coverage and keep costs down. State and Federal agencies with tower assets across the region are currently or have promised to share those assets with the MRGDC regional system as may be beneficial.

"A challenging part of the project is securing the VHF frequencies we need to be compatible and not cause or experience interference," says Peters. "We started along the border first and performed spectrum analysis at several critical sites adjacent to the Mexican border to determine which frequencies we could use."

The radios operate on narrowband digital channels, and trunking technology allows for maximum utilization of all available channels.

"The project came along at an opportune time because of the mandate from the FCC [Federal Communications Commission] to use spectrum efficient technology," Condry says. "It is important to integrate the technology. We are moving from wideband to narrowband radio channels. The fact that it’s trunked together compounds the efficiency of the system. It couldn’t have come along at a better time because we had to improve to spectrum efficiency anyway."

Another component of the project is development of a regionwide records management system (RMS) for sharing data, and providing wireless data access. Explains Condry. Agencies have been using different records management systems, at least one of which was in a shoe box. The RMS will allow users across the region to easily share information such as criminal background checks. Laptop computers using wireless data are being dispersed across the MRGDC region. Law enforcement officers use the wireless laptops to run the Texas Law Enforcement Telecommunications System from their patrol cars. The plan is for them to also have wireless access to the RMS and computer-aided dispatch.

Users in the field are adjusting to the TIP system. "We like to say around here we’ve gone from the Flintstones to Star Wars," says Anderson. "It’s been quite a change for a lot of our people."

For more information about the Technology Improvement Project, contact Joe Peters of the Border Research and Technology Center, at 514-445-5888, Joe@txsheriffs.org; Spade Condry of the Middle Rio Grande Development Council, at 839-279-4191, ext. 2036, spade@911planning.com; or Forrest Anderson, also with the Council, at 830-876-3335, ext. 1264; forest@mrgcd.org.
GOVERNANCE in Interoperability is Key to Success

If you start assembling an item by forcing a square peg into a round hole, you might end up using all of the pieces, yet still creating something that doesn’t work very well. And if you start an interoperability project by purchasing technology instead of analyzing the problems that need to be solved and coming up with a plan that involves all of the stakeholders, you might end up with a patchwork solution that doesn’t address all of your area’s problems.

According to George Ake, a retired major with the North Carolina Highway Patrol who is presently with the Border Research and Technology Center (BRTC)–Austin (operated by the Sheriffs’ Association of Texas), overcoming jurisdictions’ desire to implement technical solutions before thoroughly understanding the business needs represents one of the key challenges an agency faces in providing interoperability-related technical assistance. Kelly Harris, deputy executive director of SEARCH, the National Consortium for Justice Information and Statistics, agrees.

“It’s so much more important to figure out the business problems that need to be solved first,” Harris says. “Too often, folks hear about the latest and greatest technology and want to use it, and that so often leads to failure. You need to define the existing communication and information-sharing needs and look at it from the perspective of what needs to be accomplished. Then, you need to get the right stakeholders around the table to make that happen and get them to make a firm commitment. You next define your operational needs and last of all, apply the technology. Too often, people identify the technology without first figuring out what problems the technology needs to solve.”

“It’s a real change of paradigm,” Ake says. “People for years have just worried about their own issues. They need to realize they have to sit down, talk, and put away their differences, and to realize that all stakeholders must feel they have ownership in the solutions. It’s got to be a partnership where people work together and everybody has input in the process.”

Both Harris and Ake work for organizations that can help law enforcement agencies start the interoperability process by putting the right pieces in place first and moving on from there. Ake also provides onsite technology assistance that includes providing a notebook of samples, best practices, and models.

“I don’t tell them what to do, I tell them what has worked in other areas and might work for them,” Ake says. “Every State and area is unique and has its own political issues.”

Ake helped draft a short article, available at www.ojp.usdoj.gov/nij/topics/technology/communication/governance.htm, titled Effective Police Communications Systems Require New “Governance.” This document addresses key points in the process, including challenges to developing a governance structure and lessons learned. SEARCH also offers a number of educational materials on its website, including its popular tech guide series (http://www.search.org/programs/search-tech-guide.asp), which Harris describes as “sort of how-to manuals. There are a lot of best practices for planning and implementing information-sharing systems. We see the same trends over and over. People make the same mistakes, and the same best practices will overcome those.”

Ake has experience working in the field and with nationwide efforts as a veteran of governance development efforts with the State of North Carolina in 1996 and with CapWIN (the Capital Wireless Information Network) in 2000. He began providing technology assistance to other jurisdictions in the wake of the terrorist attacks on September 11, 2001, and believes that governance has become a major issue in the ensuing years.

“The technology is not the issue,” Ake says. “If people don’t work together and partner, you won’t get them to use the same technology. Governance is the foundation.”

To contact SEARCH, phone 916–392–2550 or visit http://www.search.org. To contact the BRTC–Austin, phone George Ake at 512–992–9971 or e-mail gake@txsheriffs.org. BRTC is a program of the Office of Justice Programs’ National Institute of Justice. SEARCH helps States develop comprehensive plans for justice information management that meet Bureau of Justice Assistance (BJA) formula grant program and other Federal reporting requirements and offers a variety of no-cost services funded by BJA under the National Technical Assistance and Training Program. More information on SEARCH and BJA can be found at http://www.ncjrs.gov/pdffiles1/bja/f0000255.pdf.

What Is Governance?

An information technology governance structure is composed of the processes and organizational mechanisms used by the enterprise to accomplish its overarching strategic goals and ideas. The governance structure can be an existing board, committee, council, or commission that has been authorized for this job, or a board, committee, council, or commission that has been created specifically to oversee the interoperability initiative. Governance can also be the shared responsibility of two or more entities or individuals.

There is no right or wrong way to build a governance structure. Governance structures can be formal or informal but tend to begin with agreements, such as memorandums of understanding, by the people who will be most affected by the structures. Governance structures can be created in a number of other ways as well, through state laws, joint powers agreements signed by agencies in separate jurisdictions or by several jurisdictions in a region, or signed charters or other agreements. Whatever the agreement, the document should be a statement of general goals that identifies the members and the decisionmaking process.

The Automated Regional Justice Information System (ARJIS) is a complex criminal justice enterprise network of 75 local, State, and Federal member agencies in California’s San Diego and Imperial counties. ARJIS has worked closely with the Office of Justice Programs’ National Institute of Justice and the U.S. Department of Homeland Security to implement a very successful Personal Digital Assistant (PDA) Mobile Project. This PDA deployment attempts to address the issues surrounding positive identification while enhancing the response to and prevention of criminal activities.

ARJIS initially deployed 100 PDAs to determine:

- Best hardware devices (battery life, keyboard, screen size, and so on).
- Most suitable applications for field access.
- Best candidates for the PDAs.
- Security and network access and compliance.
- Contract arrangements with wireless carriers.

More than 600 PDAs have been deployed, resulting in hundreds of positive identifications, arrests, and case cancellations. The ARJIS PDA project has become the cornerstone for several regional information sharing task forces in areas such as gangs, narcotics, and terrorism, as well as Downtown Walking Teams and Beach Teams.

Using the PDAs, investigators rely heavily on booking, driver’s license, and gang photos for positive identification. Investigators’ autonomy in performing data queries has proven extremely effective, allowing them to run different variations on names and license plates and get responses back much more quickly, resulting in more hits and more confirmed warrants.

Currently, participants use four different PDA models, all equipped with the Windows Mobile 6 operating system. ARJIS executes an annual refresh plan with the carriers to ensure continuous upgrade to the most current devices. Each PDA user has access to 13 applications through secure private line connections, including:

- Global Query (a single query to 12 federated databases).
- Coplink Mobile.
- California Department of Motor Vehicles and booking photos (Cal-Photo Mobile).
- Cal-Gang Mobile.
- Nets (the International Justice and Public Safety Network).
- Local warrants and wanted persons.
- Mapping.
- Access to Mexican driver’s licenses and vehicles.
- Cal-Gang Mobile, for example, provides a means for investigators in the field to identify documented gang members throughout California. Investigators have many flexible search parameters such as subject name or description, gang membership, scars/marks/tattoos (a favorite of gang investigators), and address/location. Every PDA has a built-in camera, so Cal-Gang quickly returns photos from the database with possible matches to photos taken in the field.

ARJIS is currently working on a proposal called Smart Tattoo, which would enable users of facial recognition-type applications to identify and classify tattoos. Also, ARJIS and Pacific Northwest National Laboratories, a research laboratory under the U.S. Department of Energy, are currently collaborating to design and test additional enhancements, such as:

- Tabbed browser search.
- NotesText, an application to accept exchanges of photos, videos, locations, and sketches.
- Maps with geo-based services.
- FormaField Interviews, which will include shared notes with a geo-stamped feature.
- Creation of ad hoc groups.
- Messaging between groups.

For more information, visit the ARJIS website at http://www.arjis.org/.

On April 22, 2008, a gang homicide occurred in Chula Vista, California. The victim, a gang member, was shot in the head and pronounced dead at the scene. While at the scene, the investigator immediately began using an ARJIS PDA to identify the victim’s companions, who had fled the scene and were among the only witnesses. Using the ARJIS PDA, the officer immediately identified two companions based on “monikers” provided by the victim’s family. This last, reliable information helped with the investigation.

Chula Vista Police Department
“CALCULATE’ REPEAT CRIME

After a long hard day, a resident pushes open his front door and stares in disbelief at the mess. Again. The second time in just a few days. The first time they took the television, the computer, and the stereo, but left the hunting equipment. He quickly moves toward the closet where it was stored:

Gone.

“If your house has been broken into, there is an increased risk that your house will be broken into again within a very short time,” says Jerry Ratcliffe, professor of criminal justice at Temple University. “It may be that the burglars have become familiar with the home and come back a few weeks later to get the ‘good stuff’ they couldn’t carry the first time, or they may think you’ve replaced it by then and they use their knowledge of the house to go back after the same type of items.”

New research, conducted in Australia, the United Kingdom, and the Netherlands, has found that this increased risk is transmitted to neighboring properties as well. Using funding from the Office of Justice Programs’ National Institute of Justice to build on this research, Ratcliffe used this new knowledge to develop the Near Repeat Calculator, a free software package available for download from www.temple.edu/cj/misc/nr. Users enter coordinates and dates for any type of crime, violent and nonviolent, most commonly burglaries and other property crimes. Once the data has been entered, the user receives information telling them how much the risk of another crime happening on the geographical area affected by the increased risk is higher than average.

The Near Repeat Calculator, a standalone executable program, requires no special hardware to run; it does, however, work best with high-volume crimes such as vehicle theft and burglary.

Ratcliffe cautions that this isn’t a “silver bullet” that will lead straight to perpetrators, but it does provide another valuable tool within the law enforcement crime mapping portfolio.

“This is an extensive field, an emerging field, a field that is very current in what we’re going on,” he says, giving credit to researchers such as Mike Townsley of Griffith University in Australia and Shane John of University College in London for helping to provide the foundational data on which the Near Repeat Calculator is based. This international group recently used data from the military to find near repeat patterns in improvised explosive device attacks against coalition forces in Iraq. As new research results become available, the tool will be updated, and users who downloaded earlier versions will receive an e-mail informing them that an update is available.

Intelligence-Led Policing

Professor Jerry Ratcliffe of Temple University has recently authored a book titled 'Intelligence-Led Policing,' the first book to introduce law enforcement practitioners to this emerging field.

“Intelligence-led policing is a business model and managerial philosophy where data analysis and crime intelligence are at the heart of decision-making. By using data to identify where crime is occurring, where it is likely to occur, and what the likely patterns are, law enforcement practitioners can take action to prevent crime and its negative impact on society.”

The book serves as a comprehensive guide, including the history of intelligence-led policing, how and why to do it, and possible issues. William Bratton, chief of the Los Angeles Police Department, has said that intelligence-led policing is “crimefighting that is guided by effective intelligence gathering and analysis, and it has the potential to be the most important law enforcement innovation in the 21st century.”

For more information, visit http://www.amazon.com/Intelligence-Led-Policing-Ratcliffe/dp/1843923394/
Commercial Wireless Provides Savings
Speedy Data Access for LAPD

Concerns about reliability and security have kept public safety agencies from using commercial network carriers in the past. That view is changing as technology improves and agencies begin to partner with commercial carriers for support.

One such agency is the Los Angeles Police Department (LAPD), which, with more than 9,600 sworn officers and 3,000 civilian staff, is among the largest in the nation. Covering approximately 470 square miles with a population of 3.8 million, the department must have reliable, speedy, cost-effective mobile data services. The cost of building a dedicated system to meet LAPD’s requirements would be impractical; after reviewing available options, LAPD has turned to a commercial network carrier.

LAPD uses the commercial carrier Sprint for wireless data communications in its field units. LAPD has been using Sprint since 2007 to provide data access services to 1,600 patrol cars, and thus far is pleased with the results.

“We’re very satisfied in terms of cost to use the services provided and the bandwidth availability,” says Tim Riley, chief information officer for LAPD. “We have better coverage, so that’s been extremely beneficial for us as well.”

“Sprint system has been a significant improvement in terms of data speed and resources access,” he says. “Our old network was 19.2 kilobytes per second—very small. With Sprint, we have upwards of 800 kilobytes per second. It’s huge. The download is 1.2 megabytes per second. So it’s a significant improvement in the amount of data that can be sent to the field. We can send photos and fingerprint images back and forth, and use the system for automated report writing, mapping, and access to the department intranet.” Officers also will soon have limited access to Internet sites.

The system is used for access to the California Law Enforcement Telecommunications System (CLETS), which contains information on criminal background checks, Department of Motor Vehicles information, and warrant checks, and connection with the FBI’s National Crime Information Center. The system also provides computer-aided dispatch, access to LAPD internal record systems, and access to COPLINK®, for information sharing and analysis.

For security purposes, a law enforcement agency in California that has access to CLETS must have a private connection between the agency and the data services provider.

“We use the [commercial] carrier but the service has to ride on a dedicated line. There must be a private connection because of law enforcement sensitive data,” Riley says.

The public safety community historically has had concerns about the reliability and security of commercial data services, concerns that have been alleviated somewhat as agencies begin to use commercial carriers.

“The technology has changed,” says Peter Small, program manager at the Communications Technologies Center of Excellence (CoE). “There are law enforcement agencies that are using these services and they are working well for them.” The CoE is part of the National Law Enforcement and Corrections Technology Center System, which is a program of the Office of Justice Programs’ National Institute of Justice.

With one exception last year, Sprint service has been very reliable, according to Riley.

“Last year, we had 1 day where we had an unplanned outage,” Riley says. “Sprint usually notifies us when the service will be down, usually for a few minutes when they do an upgrade. For 1 day, Sprint had a network failure. On that day, LAPD used the old system as backup. Officers can log onto either system.”

“It was a specific outage related to our DataLink services in November 2007,” says Stephanie Vinge-Walsh, a spokesperson for Sprint. “Sprint has proven to be just as reliable, if not more reliable, than the old network,” Riley says. LAPD has a solid customer relationship with Sprint, which helps when the department needs additional service.

“We work with them so that if we have a planned event, Sprint will work with us to provide more bandwidth,” Riley says. “They have portable devices to provide additional bandwidth for additional cost, so you can pay as you need it instead of paying every month for service you may not need.”

For example, in preparation for an annual immigrant rights demonstration held each year on May 1, LAPD notified Sprint that it expected more “traffic”—significant usage of the network—so Sprint could provide additional bandwidth. Traffic is the number of bits that are transferred on network connections.

Public safety agencies in the past have contracted with a vendor to build a network to be operated and maintained by the agency. LAPD built its old network at a cost of $20 million, and continues to maintain it, according to Riley. With Sprint, the agency pays about $1 million a year to have the commercial carrier available. With the commercial broadband network, LAPD pays a flat fee, with no infrastructure maintenance. The department’s monthly fee rises with each patrol car added to the service.

“In the meantime, Sprint has upgraded the network twice and we haven’t paid more,” Riley says.

“When we were considering what to do, we looked at what we had and what was in the marketplace and tried a couple of commercial carriers. Who you choose will depend on coverage, customer service, and cost,” Riley says.

For more information, contact Tim Riley of LAPD, 213-485-3100, tim.riley@lapd.lacity.org or Peter Small at the Communications Technologies Center of Excellence, 267-415-477, psmall@comtechcoe.org.
Efforts to create standards related to interoperability need to be cast in the context of an ever-changing reference, rather than as a single point forever cast in stone. Standards, like the technologies on which they are based, must evolve over time or they will stagnate. An initial standard specification may be completed, but an evolving standards process is never complete.

A standards document serves as a reference tool to describe how technology should function or how an interface should work. For example, it may explain how new technology should interface with older standards-based technology (backwards compatibility), or it can provide a vendor with a way to determine if older standards-based technology must be changed to meet the latest standard. A standard can also assist potential manufacturers in identifying intellectual property associated with a given standard.

Verifying compliance with a standard can be as simple as a vendor stating "yes our technology is compliant with standard X" during a procurement process or as complex as proving compliance as part of a comprehensive testing and acceptance regimen. A standard provides the end user, possibly a procurement officer, and the potential vendor community with a common target and a language to describe that target. If a standard is not thoroughly understood and interpreted in a consistent manner, problems will be created.

Discussed here are two important interoperability standards: Internet Protocol (IP) and Project 25 (P25).

Internet Protocol Standards

Internet protocol has become a universal technological base that affects almost every aspect of everyone’s personal and professional lives. Its many applications (such as data exchange, data and network interoperability, and wireless data) all play important roles in the overall context of public safety communications. However, even as new IP-based tools begin to resolve ongoing voice interoperability issues associated with proprietary and incompatible multivendor public safety land mobile radio systems, a lack of IP standards may mean that yet another layer of incompatible technology is being added to the mix.

"Without an agreed-upon public safety VoIP [Voice over Internet Protocol] standard, law enforcement and public safety may become entrenched in a procurement environment dominated by incompatible, single-vendor, proprietary VoIP technology," says Phil Harris, a contract senior communications engineer supporting the Office of Justice Programs’ National Institute of Justice (NIJ) Communications Technology (CommTech) program via the National Law Enforcement and Corrections Technology Center of Excellence. He explains that the public safety community needs to be aware that suppliers who claim their VoIP technology is "standards based," even if a product is entirely proprietary and therefore noninteroperable. In fact, any two competing products based entirely on "open and nonproprietary" IP standards will most likely be noninteroperable at the VoIP level because of manufacturers' design choices, whether intentional or unintentional.

In an attempt to help resolve these types of fundamental issues, a government/industry working group has created an interim multivendor standard specification that can be used to establish a minimum basis for interoperability between VoIP bridging/interconnect devices. An industry/government/public safety consensus has been reached on this profile, which will serve as a baseline foundation for subsequent revisions (now underway) to improve and build on this initial effort.

“These interim profiles allow agencies to expect minimum levels of interoperability and may lead to multivendor product sourcing. They also can provide a baseline against which compliance might be made mandatory if public funding is used to purchase VoIP interoperability technology,” Harris says.

This effort has been facilitated by the U.S. Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST), with support from the U.S. Department of Commerce Institute for Telecommunications Sciences in Boulder, Colorado. Support from many industry participants has also been fundamental to its development; NIJ technical representatives regularly attend ongoing roundtable meetings on behalf of the NIJ CommTech program.

The Bridging Systems Interface (BSI) VoIP Interface Profile is based on a collection of open standards that have been identified and adopted through the consensus process. Each must be implemented in specific agreed-upon ways to facilitate and ensure multivendor interoperability between VoIP devices. This effort will eliminate, or at least minimize, potential layers of noninteroperable technology used in critical public safety applications, Harris says.

For more information, read the following documents:

• Telephony Implications of Voice over Internet Protocol, NIJ In Short, (http://www.ncjrs.gov/pdffiles1/nij/212976.pdf).


8

IP&P25 Standards Promotion Interoperability
NCJRS is online.

Start at http://www.ncjrs.gov

The NCJRS website showcases the latest criminal and juvenile justice and drug policy information. Take advantage of:

- Topic-specific resources.
- Online registration and ordering.
- Searchable abstracts, calendar of events, and questions-and-answers databases.

Stay Informed

Register at http://www.ncjrs.gov/subreg.html to receive:

JUSTINFO. A biweekly electronic newsletter that includes links to full-text versions of printed publications.

E-mail notifications. Periodic messages about new publications and resources that match your specific interests.

NCJRS Contact Information at-a-Glance

Web: http://www.ncjrs.gov

Phone: 800–851–3420 (Monday – Friday, 10 a.m. to 6 p.m. e.s.t.)

Fax: 301–519–5212

Mail: NCJRS, P.O. Box 6000, Rockville, MD 20849–6000

The National Law Enforcement and Corrections Technology Center is supported by Cooperative Agreement #05–MU–CX–KO17 awarded by the U.S. Department of Justice, National Institute of Justice. Analyses of test results do not represent product approval or endorsement by the National Institute of Justice, U.S. Department of Justice; the National Institute of Standards and Technology, U.S. Department of Commerce; or Lockheed Martin. Points of view or opinions contained within this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance; the Bureau of Justice Statistics; the Community Capacity Development Office; the Office for Victims of Crime; the Office of Juvenile Justice and Delinquency Prevention; and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking (SMART).

Online News Summary. Online News Summary includes article abstracts on law enforcement, corrections, and forensics technologies that have appeared in major newspapers, magazines, and periodicals and on national and international wire services and websites.

Testing Results. Up-to-date listing of public-safety equipment evaluated through NIJ’s testing program. Includes ballistic- and stab-resistant armor, patrol vehicles and tires, protection gloves, handcuffs, and more.

TechBeat is the award-winning newsmagazine of the National Law Enforcement and Corrections Technology Center (NLECTC) System. Our goal is to keep you up to date with current and developing technologies for the public safety community, as well as other research and development efforts within the Federal Government and private industry. TechBeat is published four times a year.

Individual Subscriptions: TechBeat is available at no cost. If you are not currently on our mailing list, please call us at 800–248–2742, fax 301–519–5149, or e-mail us at asknlectc@nlectc.org.

Domestic Department Subscriptions: If your division, department, or agency has more than 20 individuals, we can drop ship as many copies as you require. All you have to do is provide us with the quantity needed, a shipping address and where you would like to make your payments. You’ll receive 20 or more copies of each issue. If you require fewer than 20 copies, please provide us with the names and addresses of individuals who are to receive the newsmagazine and we will send copies directly to them. Contact 800–248–2742 for additional information or to subscribe.

Address Correction: Please notify us of any change in address or point of contact. Call 800–248–2742; fax 301–519–5149; or e-mail asknlectc@nlectc.org.

Article Reproduction: Unless otherwise indicated, all articles appearing in TechBeat may be reproduced. We do, however, request that you include a statement of attribution, such as, “This article was reproduced from the Fall 2008 issue of TechBeat, published by the National Law Enforcement and Corrections Technology Center, a program of the Office of Justice Programs’ National Institute of Justice, 800–248–2742.”

Awards: TechBeat has received numerous awards, including the 1998 Best of Category, Excellence in Printing Award from the Printing & Graphic Communications Association; the first-place 1998 Blue Pencil Award for Most Improved Periodical from the National Association of Government Communicators; the 1999 Silver Inkwell Award of Merit from the International Association of Business Communicators; the APEX 2001 Award of Excellence for Magazines and Newspapers-Printed; and the APEX 2006 Award of Excellence-Newsletters-Print.

Photo Credits: Photos used in this issue of TechBeat copyright © 2008 Shutterstock; Alamy; Associated Press; Jupiterimages; Corbis; Veer; Getty Images; and Steve Kropp, images.com.

Staff: Interim Managing Editor, Lance Miller; Editor, Michele Coppola; Lead Writer, Becky Lewis; Graphic Designers, Tina Kramer and John Graziano; Contributing Writer, Phil Harris.

For help establishing an Internet connection, linking to JUSTNET, or finding needed technology and product information, call the NLECTC Information Hotline at 800–248–2742.
In addition to TECHshorts, an online, biweekly technology news summary containing articles relating to technology developments in public safety that have appeared in newspapers, newsweeklies, and trade and professional journals is available through the NLECTC System’s website, JUSTNET, at www.justnet.org. This service, the Law Enforcement and Corrections Technology News Summary, also is available through an electronic e-mail list, JUSTNETNews. Every other week, subscribers to JUSTNETNews receive the news summary directly via e-mail. To subscribe to JUSTNETNews, e-mail your request to asknlectc@nlectc.org or call 800–248–2742.

Note: The mentioning of specific manufacturers or products in TECHshorts does not constitute the endorsement of the U.S. Department of Justice, NIJ, or the NLECTC System.

Multiband Radio Trial and Evaluation Program Enters New Phase Communications Technologies CoE

In October 2007, the newly formed NIJ Communications Technologies Center of Excellence launched a program to evaluate multiband radios (single radios that access more than one band, such as UHF and VHF) to assess their costs and potential benefits for law enforcement operations. Conducted in partnership with the Oranjetown (New York) Police Department, the program has deployed several multiband radios during actual police operations, including a recent accident in which a multiband radio coordinated resources to assist several injured police officers.

“There are a number of hardware vendors who are claiming they can provide a single portable police radio that can access the multiple bands used by law enforcement, such as VHF, UHF, and the higher frequency bands presently used for communications,” explains Rick Mulvihill, CoE deputy director. “Should these radios continue to perform as advertised, this will significantly alter the competitive landscape and broaden the range of purchasing options for the criminal justice community.”

Based on the initial results, the program moved on to a new phase, incorporating equipment from other vendors into the test program under Orangejtown’s experimental radio license issued by the Federal Communications Commission.

“We believe police radios with these characteristics will emerge from multiple vendors as viable options for law enforcement over the next 2 years,” Mulvihill continues, “and we want to make sure the practitioner community understands both the opportunities and the challenges.”

For more information, contact Rick Mulvihill at 267–415–4761 or rmulvihill@commtechcoe.org.
Offering no-cost assistance to law enforcement and corrections agencies and crime laboratories—large or small, rural or urban—in the implementation of current and emerging technologies, the National Law Enforcement and Corrections Technology Center (NLECTC) System is an integrated network of centers, specialty offices, and criminal justice technology Centers of Excellence located across the country.

Established in 1994 by the Office of Justice Programs’ National Institute of Justice (NIJ) as part of its research, development, testing, and evaluation initiatives, the NLECTC System serves as an “honest broker” resource for technology information and assistance and helps introduce technologies into practice within the criminal justice community.

The NLECTC System seamlessly delivers its expertise to the Nation’s 19,000-plus police agencies; 50 State correctional systems; thousands of prisons, jails, and probation and parole departments; and crime laboratories in a number of technology areas. These technology areas are supported by technology partners who provide the leveraging of unique science and engineering expertise. In addition, technology working groups and a national advisory council provide guidance relating to the technology needs and operational requirements of the public safety community for NIJ’s various technology focus areas and ensure a focus on the real-world needs of public safety agencies.

Contact NLECTC for:

Technology Identification
The NLECTC System provides information and assistance to help agencies determine the most appropriate and cost-effective technology to solve an administrative or operational problem. We deliver information relating to technology availability, performance, durability, reliability, safety, ease of use, customization capabilities, and interoperability.

Technology Assistance
Our staff serves as proxy scientists and engineers. Areas of assistance include unique evidence analysis (e.g., audio, video, computer, trace, and explosives), systems engineering, and communications and information systems support (e.g., interoperability, propagation studies, and vulnerability assessments).

Technology Implementation
We develop technology guides, best practices, and other information resources that are frequently leveraged from hands-on assistance projects and made available to other agencies.

Property Acquisition
We help departments take advantage of surplus property programs that make Federal excess and surplus property available to law enforcement and corrections personnel at little or no cost.

Equipment Standards and Testing
We oversee the development of performance standards and a standards-based testing program in which equipment such as ballistic- and stab-resistant body armor, double-locking metallic handcuffs, and semiautomatic pistols is tested. NLECTC also conducts comparative evaluations (testing equipment under field conditions) on patrol vehicles; patrol vehicle tires and replacement brake pads; and cut-, puncture-, and pathogen-resistant gloves.

Technology Demonstrations and Capacity Building
We introduce and demonstrate new and emerging technologies through special events, conferences, and practical demonstrations such as the Mock Prison Riot™ and an annual public safety technology conference. We also provide hands-on training assistance for the latest technologies through workshops and software programs dealing with crime mapping, community corrections, and critical incident management. In addition, on a limited basis, NLECTC facilitates deployment of new technologies to agencies for operational testing and evaluation.

Technology Information
NLECTC disseminates information to the criminal justice community at no cost through educational bulletins, equipment performance reports, guides, consumer product lists, product information databases, news summaries, meeting/conference reports, videotapes, and CD–ROMs. Most publications are available in electronic form through the Justice Technology Information Network (JUSTNET) at www.justnet.org. Hard copies of all publications can be ordered through NLECTC’s toll-free number, 800–248–2742, or via e-mail at asknlectc@nlectc.org.

Technology Product Network
The Technology Product Network (TPN) provides one-stop access to information on currently available products for law enforcement and corrections. Vendors and technologists who register with the TPN can upload information about their products, while registered practitioners can participate in discussion forums about the products found in the database. Registered users also receive e-mail notifications of new products that match their specified interests. Visit the TPN website at www.technetwork.com.
P25 Compliance Assessment Program

P25 defines a suite of standards for public safety digital wireless radio communications systems to allow multiple vendors to supply products and services that will interoperate with each other.

In partnership with DHS’s Project SAFECOM and with support from NIJ’s CommTech program, the NIST Office of Law Enforcement Standards (OLES) began to develop the P25 Compliance Assessment Program in 2005. The program’s central purpose is to help emergency response officials, including law enforcement, make informed purchasing decisions. By consulting a list published on the Responder Knowledge Base (www.rkb.us), officials will know which products have passed an established testing protocol developed under NIST oversight.

The program has three parts: a supplier declaration of compliance (SDoC), a summary test report, and a records and inspection provision. The SDoC is a formal manufacturer declaration of product compliance that provides details about product configuration and lists the types of tests applied to the product and test results, and also includes the signature of a responsible company official. The summary test report contains more details about the tests in a uniform, easy-to-review format. Finally, manufacturers are required to maintain all records of the test results, which are open to inspection by NIST representatives. Achieving the compliance assessment vision in full will take years, but NIST expects to begin implementing aspects of the program in fall 2008.

The P25 Compliance Assessment Program allows manufacturers to develop their own laboratory compliance programs, thus avoiding the need to train employees of outside laboratories. Throughout the early stages of the Compliance Assessment Program, NIST and vendors expect there to be growing pains. From time to time, both standards and procedures will be modified to resolve problems stemming from inconsistent interpretations.

“Radio systems of the past were primarily hardware-only products, but systems today depend on both hardware and software components. Consequently, legacy equipment and software upgrades, which can cause problems for smoothly functioning interoperable communications systems if not perfectly compatible with all equipment in the system, will pose a continuing challenge,” says Dereck Orr, NIST program manager for public safety communication standards. “To cope with the inevitable growing pains, NIST will try to get feedback from industry representatives and others and use it to sharpen both testing procedures and the standards themselves.”

Orr continues that participation by manufacturers is strictly voluntary: “They may develop, market, and sell P25 products without participating in the compliance program, which is similar to NIJ’s well-known body armor testing compliance program. However, DHS will restrict, aside from a few special considerations, its grants for purchasing equipment to products that appear on its published list. Manufacturers’ most detailed test reports and anything proprietary may remain confidential; only facts and data documenting compliance must be released.”

Project 25 was launched in 1989 to develop standards that define how digital land mobile radio systems should operate and how key system interface standards would allow radios and other components to interoperate regardless of manufacturer. The ultimate goal of P25 is to specify formal standards for eight interfaces between the various components of a land mobile radio system:

- Common air interface.
- Inter-RF subsystem interface.
- Fixed station subsystem interface.
- Console sub-system interface.
- Network management interface.
- Data network interface.
- Subscriber data peripheral interface.
- Telephone interconnect interface.

For More Information
For more information, visit the “Project 25 CAP” section of the SAFECOM website: http://www.safecomprogram.gov/SAFECOM/currentprojects/project25cap/project25cap.htm. To cope with the inevitable growing pains, NIST will try to get feedback from industry representatives and others and use it to sharpen both testing procedures and the standards themselves.”

Orr continues that participation by manufacturers is strictly voluntary: “They may develop, market, and sell P25 products without participating in the compliance program, which is similar to NIJ’s well-known body armor testing compliance program. However, DHS will restrict, aside from a few special considerations, its grants for purchasing equipment to products that appear on its published list. Manufacturers’ most detailed test reports and anything proprietary may remain confidential; only facts and data documenting compliance must be released.”

Project 25 was launched in 1989 to develop standards that define how digital land mobile radio systems should operate and how key system interface standards would allow radios and other components to interoperate regardless of manufacturer. The ultimate goal of P25 is to specify formal standards for eight interfaces between the various components of a land mobile radio system:

- Common air interface.
- Inter-RF subsystem interface.
- Fixed station subsystem interface.
- Console sub-system interface.
- Network management interface.
- Data network interface.
- Subscriber data peripheral interface.
- Telephone interconnect interface.

For More Information
For more information, visit the “Project 25 CAP” section of the SAFECOM website: http://www.safecomprogram.gov/SAFECOM/currentprojects/project25cap/project25cap.htm.