International City/County
ICMA
Management Association

IQ
SERVICE REPORT

VOLUME 32/ NUMBER 1 JANUARY 2000

INFORMATION AND COMMUNICATIONS TECHNOLOGY FOR PUBLIC SAFETY

Few public services can be so thoroughly revolutionized by the advent of high technology as public safety services. In all areas of public safety, from communications to record keeping to response planning and management, new computer-based technologies offer the potential for much better service at greatly reduced cost.

Whether these technologies will be used to best effect depends largely on the foresight and understanding of local appointed and elected officials. The promise of better service at lower cost is only a promise unless basic practices and procedures are adapted to take advantage of new ways of acquiring, sharing, and storing information.

This report describes information and telecommunications technologies that have applications for public safety and discusses implementation issues for each. Case studies from the following jurisdictions illustrate the benefits of interagency and interjurisdictional cooperation:

- Oklahoma County, Oklahoma
- Washington County, Oregon
- Mankato, Minnesota, and neighboring jurisdictions.

International
City/County
ICMA
Management
Association

ICMA's
InQuiry
Service

VOLUME 32 / NUMBER 1
JANUARY 2000
ITEM NUMBER E-43009

ICMA's IQ Service Reports (ISSN:0047-5262) are published monthly by ICMA, 777 N. Capitol St., NE, Suite 500, Washington, DC 20002-4201. © 2000 by the International City/County Management Association. No part of this report may be reproduced without permission of the copyright owner.

These reports are intended primarily to provide timely information on subjects of practical interest to local government administrators, department heads, budget and research analysts, administrative assistants, and others responsible for and concerned with operational aspects of local government.

IQ Service Reports are published as part of ICMA's InQuiry Service subscription package. The package also includes unlimited access (via the Internet or staff-assisted searches) to ICMA's InQuiry Service—a database of thousands of local government reports, budgets, ordinances, program descriptions, purchasing manuals, job descriptions, and other materials—a bimonthly subscriber newsletter, information packets, and a number of other valuable ICMA publications. Requests for general information concerning ICMA's InQuiry Service subscription package should be addressed to Bruce Thibault at 202/962-3587, or bthibault@icma.org

IQ Service Reports
Rita Soler Ossolinski, *Director*
Michele Frisby, *Deputy Director*
Bruce Thibault, *IQ Service Coordinator*

Publications
Barbara H. Moore, *Director*
Christine Ulrich, *Senior Editor*
Dawn Leland, *Production Director*
Elissa Fitzgerald, *Layout*

Recent Reports

12/99	Media Relations: The Manager's Role
11/99	Work-Life Balance: Integrating Benefits with Expectations
10/99	Water and Wastewater Services: Meeting Current Challenges
9/99	Land Use Decisions: Assuring Fairness
8/99	Volunteer Programs in Cities and Counties
7/99	The Role of the Public Library
6/99	Multiyear Budgeting
5/99	Preventing Workplace Violence
4/99	Smart Growth for Local Governments
3/99	Introduction to Infrastructure Financing
2/99	Wetlands and Watersheds: Six Case Studies
1/99	Managing for Continuous Improvement: Chesterfield County, Virginia

Information and Communications Technology for Public Safety

Tim Dees, the author of this report, is a former police officer and college instructor in criminal justice. He has served as a trainer and consultant on technology issues to a number of public and private concerns and writes a monthly column on computers and technology for Law and Order *magazine. He is the author of a book on the use of the Internet in law enforcement,* Online Services for Law Enforcement *(to be published by Prentice-Hall). He can be reached at 706/235-8104, or by e-mail at dees@compuserve.com.*

As the gatekeeper of the local government coffers, the city or county administrator is drawn in many directions. Every department head has a list of excellent, well-thought-out budget requests, many of them for technology. Because technology progresses so rapidly, it is almost a full-time job to keep up with what particular products can do. An uninformed manager may find out many months down the contractual road that the purchased "asset" is not nearly as suited to the task as was represented. Thousands, and possibly millions, of dollars are wasted, and the governing council or commission is unlikely to give its blessing for another purchase. The phrase "good money after bad" usually comes up sometime during this discussion. In short, knowing something about available technology may be critical to the professional survival of a public administrator.

This report provides an overview of some of the technologies presently available, and on the horizon, for public safety applications. The report is intended mainly for managers in small and medium-size local governments. Large governments often have full-time technology consultants available to them, and have the budgetary clout to command that products be created especially for them. Most local governments do not have these luxuries, and must depend on a biased vendor to tell them what might work and what might not (the latter almost always being the competitor's product).

This report will address several of the technologies and applications available to improve the quality and efficiency of public safety operations, including

- Trunked radio systems
- Global positioning satellite systems
- Wireless data strategies
- Cellular telephone technology
- Digital records systems
- Intelligence analysis and expert systems
- Electronic and voice mail

The report also addresses the impact that technology can have on the workforce, your most precious and costly resource. A wise man once said "Computers work—people should think." Technology will not do employees' jobs for them, but it can help them to do their jobs better and more efficiently.

WHAT DO YOU NEED?

Community Profile

In choosing among technologies, the manager must first consider the composition and situation of the community. For instance, a coastal community that is threatened by seasonal weather problems (hurricanes, windstorms, floods) may be at greater risk of losing electrical power for a prolonged period than one in a suburban area. When power is lost, resources on which public safety depends (communications, electrical gasoline pumps, lighting, heating and cooling, etc.) can become inoperable, and alternatives have to be considered. Certain radio systems work better in rural environments than in dense, urban settings. Communities that share borders with one or more other communities may be able to pool resources to save costs, while more isolated communities do not have this option.

> **The small community may be one of the best places to use technology to extend thin personnel resources.**

In smaller communities, common objections to technology acquisitions are that new "gimmicks" waste taxpayers' money and that such innovations have no place in a small town. In fact, the small community may be one of the best places to use technology to extend what are usually thin personnel resources. Of the more than 17,000 law enforcement agencies in the United States, 78 percent have fewer than 24 officers, and over 1,000 of these have only one full-time or part-time officer. This means that some agencies are not able to provide patrol services 24 hours a day, and when services are provided, only one officer is on the street.

In this scenario, it makes good sense to extend that officer's capabilities with state-of-the art communications and information processing technology, so that his or her time can be spent doing the job for which he or she is trained and qualified—not driving to and from the station, filling out forms, or trying to obtain information. Technology cannot replace people, but it can greatly augment their capabilities. Moreover, technology is usually a one-time investment, whereas manpower is a recurring cost that can quickly get out of control.

Public Safety Mission

The public safety mission varies from one community to another. Some communities, for instance, maintain their own professional emergency medical services (EMS), but others provide EMS through private agencies, a volunteer medic corps, or hospital services. Some communities may not have a law enforcement component, replying on another governmental agency (such as a county sheriff's office) to provide law and order functions. There really isn't any such thing as a universal application for technology, given the diversity in the makeup of public safety missions.

> **It is wise to assemble representatives from all public safety entities to review any proposed purchases of technology.**

What is important is that public safety, however it is administered, be considered as a whole, rather than by its components. Sooner or later, the components have to work together, and incompatible systems waste resources and lead to inefficiency. The current popular term for compatibility among systems is "interoperability." High-tech systems are plagued by a lack of interoperability, because the operating systems and underlying infrastructures often represent years of costly research and development, and the firms that make the investment in these projects want to protect their proprietary interests.

Because a new system that solves one problem may create new problems if it is unable to share resources with an existing system, it is wise to assemble representatives from all public safety entities to review any proposed purchases of technology, even if the purchase appears to affect only a single agency. For instance, an evidence tracking system for the police department might appear to affect only that department. However, if the fire department has a role in bombing or arson investigations, fire personnel may be involved in the collection or processing of evidence, or even have primary responsibility for arson investigations. Leaving the fire department out of the loop when obtaining a new evidence tracking system can be counterproductive.

Bringing representatives from different agencies to the table to consider a major capital purchase of technology may actually build some bridges, as they come to better understand one another's missions and problems.

Communications

Of all the areas where technology can be applied to enhance public safety, communication probably provides the most "bang for the buck" and also the greatest number of options. Fifty years ago, two-way radio communication revolutionized the way that public safety providers did their jobs. No longer tied to the station or to an inflexible signal box system to transmit information between headquarters and the field, police, firefighters and medics could dynamically redeploy at a moment's notice, and could communicate with one another for mutual support.

In the early days, the person at the base station end of the radio was frequently another officer, firefighter, or medic, who had little if any skill at managing units or communications traffic. Now, in most places, the communications operator is a vital link in the public safety community, and the job is often a career choice. The use of technology in public safety communications has created a specialized niche for people proficient in the operation of radio transmitters and receivers, computer databases, crisis and resource management, basic emergency medical skills, and the complexities of computer-aided dispatch (CAD) software.

Because most public safety incidents begin with a message to the communications center, this is the logical starting point for planning an information database. A truly integrated information system will record the data produced at the first call and pass that data on to the other components of the system. If this is not done, then there will inevitably be duplication of data entry and the possibility of the introduction of errors.

Other technology applications that affect the communications function are global positioning satellite (GPS) tools, trunked radio communications systems, internal communications systems (pagers, voice mail, e-mail), methods of geographically locating callers using cellular phones, and voice data logging systems.

Public Safety Functions

Patrol/community policing. Few public safety employees are as visible or as accessible as the uniformed patrol officer. Recent innovations such as foot patrol, motorcycle patrol, bicycle patrol, mounted (horseback) patrol, air support, waterborne patrol, and even patrol on in-line skates have been used to bring the officer into closer contact with the community.

The basic equipment required to outfit a patrol car used to be a two-way radio, a rotating or flashing warning light, a siren, and some distinctive markings. These accessories alone add 10 to 25 percent to the cost of the basic stock automobile, which is usually a large-capacity “family” car with the largest engine and best cooling, braking, and electrical system available.

The modern patrol car still has all of these components, but often adds a traffic radar or laser system, a mobile data terminal (MDT), an in-car or officer-borne video recording system, equipment to contain hazardous materials spills, traffic cones and/or flares, a first aid kit, a fire extinguisher, night vision equipment, a shotgun and/or patrol rifle, and other miscellaneous gear. The modern patrol car can represent an investment of well over $50,000 for the local government that owns it, and much of that equipment can be destroyed if the car is wrecked, or stolen if the car is left unattended.

Officers who don’t patrol in vehicles also need equipment. A bicycle patrol officer may not be able to carry a video recording system or a shotgun, but there is technology available that can give him or her some rudimentary benefits of an MDT, and there is no reason for any officer on duty to be out of communication at any time.

Some departments equip police officers with communication devices that they can use while off duty. Police officers usually have the option of being armed while off duty, and they may elect (or be expected) to intervene in crime situations that they happen to witness while not on duty. When this occurs, the officer is at a profound disadvantage if he does not have the resources of his patrol car available, and can’t communicate with the dispatch center and other on-duty officers. If the officer intervenes in a way that results in injury or death to a suspect or bystander, then the local government will almost certainly be the defendant in a costly civil action. Off-duty communication devices don’t eliminate this risk, but they can provide officers with an alternative to using force when intervening in an incident.

Criminal investigation. The criminal investigation function varies significantly from one law enforcement agency to another. Some law enforcement agencies have only one or two people assigned to this function, and it may be a collateral duty merged with supervision or patrol. In these agencies, the same technology that can augment the patrol function is generally applicable to investigations. When there are many investigators, or when investigations span several agencies, or when investigations are complex, criminal intelligence software can be very useful. Internal communications systems, such as electronic mail, pagers, and voice mail, can also help in these environments.

Corrections. Software for managing the corrections function, especially when it is integrated with other systems and components, can reduce the liability potential for local governments by more fully documenting the intake, care, movement, and custody of inmates. The same software can increase the safety margin for correctional personnel, by making more information, and more current information, concerning inmates immediately available.

Fire prevention and suppression. In most communities, the fire department is responsible not only for fire suppression, but also for rescue work, getting people out of wrecked cars and collapsed structures, responding to hazardous materials spills, and sometimes for emergency medical services. A fire company responding to an alarm has little time to find out what materials may be located inside the burning structure, and the lack of that information can be disastrous. Some materials react with water to produce noxious gases or explosions, and firefighters who enter a burning structure where chemicals are stored may be quickly overcome if they are not wearing the appropriate protective gear.

Most fire agencies do an admirable job of training their employees in the handling of hazardous materials, but they may not always know where those materials are stored in their communities. Mobile data terminals like those in patrol cars can display information from databases of hazardous materials storage, as well as contact names and numbers for the people responsible for these materials. These same terminals can display floor plans of buildings to help firefighters search efficiently for citizens and special hazards.

Emergency medical services (EMS). The model for information and communications technology for EMS is very similar to that for fire services. EMS personnel have to respond to locations rapidly and at a moment’s notice, and often they will be working closely with police and fire units. Hazardous materials issues are important for EMS workers, for their own protection as well as for the protection of their patients (who may include the fire and police responders). EMS units can also use mapping and routing software to help them respond to incidents and floor plans to locate a particular office or room in a structure. Both volunteer firefighters and volunteer EMS units need similar technologies.

Disaster management. Local governments cannot do much to prevent a disaster, but they can minimize its impact by preparing for it and managing the damage once “the dust is in the air,” as the professionals like to say. Disaster management requires that the planners assume any commonly available resource may become unavailable, and allow for reserve supplies or contingency plans. Computer software can simulate the spread of a chemical, biological, or radiological agent in the atmosphere or inside a structure, and show the propagation of the toxic "plume" under the effects of wind, rain, application of fire retardant, or some other effect that could speed or slow the spread of the agent. Other software packages allow an incident commander to track and log the activities of response units so that they aren't overlooked, and provide a record for documentation and training purposes later.

INTEGRATED PUBLIC SAFETY SYSTEMS

"Integrated" information systems that track incidents and data from the start of an incident until the closure of the case, and share data between governmental entities, have many advantages. First, because an integrated system pulls data from multiple sources, many of the problems caused by duplication of effort and noncommunication are avoided. When information is disseminated informally within a public safety agency, the process is inefficient and there is always someone who doesn't get the word.

> **Information is available to everyone who needs it as soon as it has been entered into the system.**

Commonly, information about a single person, place, or event is entered at several locations, by different persons, and at different times. Computers read data literally and can't associate "Bill Green" with 'William Green," "Billy Green," "Wm. Green," or "W.M. Green," as a person might. Criminals often change their names, dates of birth, and social security numbers slightly with each police contact, so that outstanding warrants, probation violations, and prior convictions won't be detected. Fingerprints will identify individuals positively, but most agencies use "inked" fingerprint cards (called ten-print cards, because the impressions of all ten fingers are taken), which have to be mailed off to the state or federal records repository, classified, and matched with existing records. Only then can the law enforcement agency that submitted the ten-print cards be advised of the true identity of the person arrested, and this process routinely takes three months or more. By that time, the subject has been released from jail, and if he is smart, he is long gone.

An arrestee's identifying information (name, date of birth, social security number) may be entered into various terminals many times during the progress of his case through the police department, jail, and court systems. With each entry, there is the potential for a typographical error, a misstatement of information, or some other error that will cause the records to be mismatched. Mismatched records lead to missed court appearances, accidental release of inmates, and wasted time and effort for everyone.

Integrated systems also reduce the amount of paperwork created, which reduces costs. It may cost as much as two dollars to handle a paper form.[1] An integrated system eliminates most of the paper forms altogether, and keeps data from initial entry, passing information along from one step to the next.

Another significant advantage of an integrated system is that information is available to everyone who needs it as soon as it has been entered into the system. The chief of police and the public information officer don't have to wait for the records bureau to make a copy of the arrest report to see what has gone on—they can pull the information up directly.

Just as important, while everyone who *needs* access to the information can get it, those who don't have the proper authorization can't get access. If certain data must be kept confidential, there is no need to cover portions of a form before a copy is made, or read information to a third party from a computer screen. Custom reports containing the information that each user wants and needs can be created for every level of authorization. A record can be created for every access of any information, to discourage or detect subversion or misuse of the system.

Despite these advantages, two factors weigh against integrated systems: money and politics. These systems don't come cheap. A network infrastructure has to be built if it is not already in place, hardware has to be purchased, and the software has to be customized for the purchaser. The potential for long-term savings is good but the initial price tag is high.

A second obstacle to an integrated system can be organizational conflict or hostility. There can also be significant infighting over who is going to be "in charge" of the project, and subordinate agencies may fear that they will be denied some advantage.

Some funding issues may be ameliorated with federal grants. Grants available through the U.S. Department of Justice are addressing cooperation and communication among public safety agencies, particularly those in rural areas with the objective of helping them prepare for terrorist threats. If the entities involved in an integrated system can come together to apply for one of these grants, they may have a much better chance of getting funding than they would if they apply for funding as individual agencies. Integrated systems that enhance the ability of agencies to work together across jurisdictions and "turf" are far more likely to be funded than stand-alone systems that serve a single agency (see the sidebar on page 7).

Integrated justice information system

Oklahoma County had a problem. The county, which is Oklahoma's most populous and includes Oklahoma City, was using mainframe, COBOL-based systems that weren't Y2K compliant for their public safety functions, and it looked as though it would be prohibitively costly to upgrade them. Moreover, systems and data were fragmented, so that employees couldn't readily access information that they needed to work safely and efficiently.

For example, the sheriff's office had no quick way of determining whether an inmate due for release had new arrest warrants outstanding, because the court, prosecutor's office, and jail systems couldn't "talk" to each other. Employees at the reception desk, fielding calls and visits from inmates' family members and bail bondsmen, had to telephone other employees to determine the status of an inmate, and sometimes several calls were required to get all of the information required.

The county looked at integrated systems in the public safety marketplace and chose E*Justice System™, a TRW product that had been successfully implemented in McLean County (Bloomington), Illinois, and offered interoperability between agencies.

Commenting on the organizational barriers that often make it difficult to adopt one system to serve several political entities, John Whetsel, sheriff of Oklahoma County, said, "The cost savings benefits were obvious from the beginning, and that made sense to every administrator involved in the project. The biggest concerns were voiced by the MIS people, who were concerned with access and security issues. Once they saw the product, they were fully supportive."

Like most integrated systems, E*Justice emphasizes modularity, so that customers don't have to buy functionality that they don't need or can't afford. As needs and budgets evolve, more modules can be added, with very few changes or interruptions for ongoing users.

Conversion of existing data to a format that E*Justice could handle proved to be the biggest challenge during implementation in Oklahoma County. It took nine months of work with the county's various databases to get them into a consistent format. A mobile data capability was added to the system in a second phase, allowing incident reports to be filed directly from the patrol cars in the field and permitting computer-assisted dispatching functions from the car-based laptops as well as access to the message switches for the county, state, and national criminal justice information databases.

In Oklahoma County, the emphasis in installing the new system has been on improving communication between the sheriff's office, the prosecutor's office, and the courts. For instance, inmate tracking had been a problem, because of the inmates' practice of impersonating one another to gain release or privileges. Deputies in charge of releasing inmates now see a mug shot of the inmate displayed on a terminal while completing the release information, reducing the likelihood that the wrong inmate will be discharged. The information system automatically checks with the court and prosecutor's databases to ensure that there are no holds on the inmate that might have been created while he was in custody.

Deputies supervising inmates in the housing units can look at a display of inmate names and mug shots that follows the layout of the housing units, to help them make sure that each inmate is in the right cell. When inmates are fingerprinted, using the county's LiveScan/AFIS system, the scanned fingerprints are stored in the E*Justice system (this information was kept in an entirely separate database previously).

A new enhancement to the system is portable fingerprint readers. The county has purchased six portable fingerprint readers, and the software is in final development. All fingerprints of current inmates (who number approximately 2,200) will be downloaded each day into the readers. When any movement is made or medication given, a fingerprint check will be made on the portable readers, which will verify the identity of the inmate. There will be readers at the releasing window, court security, medical, and other critical places in the jail, and additional units will be added later.

The integrated justice information system may increase county revenues. Oklahoma County's jail, like many other jails, houses inmates from other jurisdictions when those agencies lack facilities or space for detention. The county charges the contracting agency a boarding rate that varies with the agency and the type of supervision required. E*Justice tracks these costs automatically and generates bills for the sheriff's office to send out to their contractors. Inmates' commissary trust accounts are also maintained, eliminating the need for inmates to have cash or even credit certificates in their control.

Several of the municipalities in Oklahoma County have expressed interest in plugging in to the county system. They could then share data across the network and integrate their public safety data with the county's, making local government operations even more efficient. In this way, a state-of-the-art information system becomes accessible to small governments that would never have considered it because of budgetary restrictions.

Sheriff Whetsel summed up the most important factor in implementing an integrated system across multiple entities: "Support for the project has to be at the top. Once the top administrators are committed to the project, everyone else will find a way to make it happen."

CHOOSING TECHNOLOGY

When the time comes to choose technology, you can devote yourself to the study of technology in the area of your intended application, or you can hire a consultant to advise you in your acquisition and purchase. Other local governments that have made similar purchase decisions can provide information about consultants.

You should also ask your contacts in other local governments how they solved problems similar to yours. Most reputable vendors encourage you to discuss their product with past and current customers. Several major vendors post lists of their customers on their Web site.

When a new information system must interface with existing information systems, the product's track record is critical, and most public safety systems are in this category. Every state has a statewide database of criminal justice information that contains information on fugitives, criminal histories, firearms registrations, license and permit information, and other data necessary to day-to-day law enforcement.

> **You must see the system that you are purchasing operating in a real-world environment.**

In addition to these databases (and often integrated with them), states maintain data on motor vehicle registrations and drivers license records, which are also critical to law enforcement operations. These state systems are constructed or configured in a variety of ways. One state lists all citizens who hold permits to carry concealed firearms in a central database; another maintains these records only in the courthouses of the county that issued the permit. Some states allow a search of the database to see what motor vehicles are registered to a particular person; others allow a search only by license plate or vehicle identification number. The format of each report or result is different. Although all these systems handle similar data, they are not configured with consistency.

Whatever method you choose to select a vendor, you must see the system that you are purchasing operating in a real-world environment, in a setting as close as possible to the one in which you will use it. Systems developers often use their early customers' sites as test beds for new technology, and devote first payments to further research and development. You need to know if the system you are buying is tangible and working, or whether it exists only on the vendor's drawing board.

Budgetary Considerations

New technology is always expensive, because developers have to recoup the costs of their research and development. The newer the technology, the more expensive it is. And, when a new system is introduced, the old system often has to be scrapped. You're lucky if the old system is a box of file cards or a legal pad attached to a clipboard. More often, the old system is one that cost a great deal of money when it was purchased, and at least one member of the city or county commission will remember just how much the old system cost.

You must also consider the speed with which technology changes, in budgeting for a major new system. Just as home computers become outdated in six months, so do cellular phones, radios, and software used in the public safety arena.

In addition, if the environment where the technology is going to be used is likely to change significantly, then it may be necessary to upgrade or increase the capacity of the system when needs change. For instance, if the size of your public safety force increases, you may have to add capacity to your trunked radio system or revamp the system. Long-term planning and realistic projections of growth are important in making a technology purchase.

Systems Integrators

A systems integrator selects components from several vendors and merges the components to produce a complete system. The systems integrator may include some of its own products in the final system, or it may not. For instance, when a county contracts with the XYZ Corporation for a countywide criminal justice information system, XYZ may select a wireless component for communication with units in the field from one vendor, fingerprint scanners from one hardware supplier, terminals and computer processors from another supplier, and software from one or more software vendors. The finished system, with components from many vendors, carries the name of the XYZ Corporation on the faceplate. More important, the county's check is written to the XYZ Corporation.

Ideally, the systems integrator chooses the best quality components from the best providers and makes all of the components talk to each other. Ultimately, the systems integrator can be held responsible for the entire delivered product, relieving the customer from the unpleasant job of negotiating fixes with each of the subcontractors.

If your project requires special expertise, then contracting with a systems integrator may be a wise choice. Just remember that a good systems integrator will charge a premium fee for doing these intermediary tasks.

Personnel Issues

Your employees have to learn to use the new technology effectively if it is to be effective. Most line employees will support the acquisition of technol ogy, because there is a general perception that technology makes work easier and improves the status of the job. Introducing technology into the workplace can also be an acknowledgment by management that a job is difficult, and that the employee can benefit from some additional help.

Unfortunately, some employees feel threatened by technology. An employee who sees the introduction of new technology as shifting power, status, or authority away from himself is likely to resist or subvert the project. For example, a new information management system can make the department less dependent on the person who has been the primary keeper of records and cause a perceived loss of status. Other employees may fear that they will not be able to master the new system, or that someone will have a better command of the new technology than they have of the old.

To win the support of your work force, it is essential to involve the employees who will use the new system and be affected by it, from the inception of the project. An advisory committee that has no definitive input into the planning and implementation of the project is not enough. Line employees need to participate in every stage of the project with a voice equal to that of the most senior person in the process. The people who will use the system probably know a lot more about the task than their managers. Even managers who come "up through the ranks" tend to lose touch with the everyday demands of the job. Line employees working at the job where the new system will be implemented will be the best qualified to advise on parameters and requirements for the system when the request for proposals is being created.

Some local governments identify an employee with some computer expertise and assign him or her to use existing software and equipment to create a low-cost, homegrown database or other application. This is almost always a bad idea. People who are not professional software developers usually don't document their work properly. They are then the only people who can modify the code or repair a problem, and they are the only ones who can modify the system to meet additional needs. The format of the database may be non-standard, so that the existing data will not export smoothly when a succeeding system is brought on line. Finally, the local government's information is in the hands of a single individual. Contented employees don't always remain contented, and people can commit rash acts when they are angry, wiping out or altering records on a whim. Don't allow one person to hold all of your information hostage.

On the positive side, employees who are involved in the planning, selection, and implementation of a technology application will be the best possible cheerleaders for the new system. They will inform people about the capabilities and limitations of the system, and they are probably the best choices for peer "gurus" or trainers for other employees who will need to learn to use the system.

Some employees are more technically oriented than others. These employees usually identify themselves by their hobbies, lifestyles, or backgrounds. The public manager can draw on these employees to advise on technology acquisitions and to assist in introducing other employees to the new systems. The employees best qualified for this kind of assignment may not be ideal employees from the conventional point of view. People with strong technical skills sometimes relate better to machines than they do to people and might not be as outgoing as some others, but bringing their interests and skills to bear on the problem of acquiring new technology may be one of the best ways to get them more involved (and accepted) in the mainstream of the organization.

Technology changes the workplace in ways that we often fail to anticipate. At the start of the 1990s, no one would have understood the significance of a line of text at the bottom of an advertisement that started out "www..." Electronic communication draws us closer together in many ways, but it also isolates us, since some employees now use e-mail to communicate with colleagues they would previously talk to at lunch. Be aware that new technologies will also affect the way that your employees view their jobs, and the way they view each other. Choose your tools carefully.

Federal funding

The federal government can provide substantial assistance in the form of grants for technology purchases for public safety. At this writing, community responses to acts of terrorism, cooperation between local government agencies and federal entities, and domestic violence are "hot topics." The Department of Justice's National Law Enforcement and Corrections Technology Center (NLECTC), has both a mailing list and a Web site that posts announcements of grant opportunities and hardware that can be transferred from federal to state ownership. Contact the Office of Science and Technology, National Institute of Justice, 810 7th Street, NW, Washington, DC 20531; 202/307-0645; http://www.nlectc.org.

AVAILABLE TECHNOLOGIES AND WHAT THEY DO

Trunked Radio Systems

Public safety agencies are prolific users of the available radio spectrum, and the demand for bandwidth has increased substantially in the last 20 years. Radio channels are used to transmit clear and encrypted voice messages, digital data, pager messages, cellular telephone traffic, and every other type of information conceivable. The frequency bands reserved for these communications are increasingly crowded, and licenses for new channels are extremely difficult to obtain.

One way to alleviate crowding on the radio spectrum is to use trunked radio systems. A trunked radio system is a computer-controlled network that uses a range of channels reserved for the entire system. When a user presses the transmit button, the radio sends a signal to the base station that tells the system that this particular user wants to talk. The system then searches for an available clear channel and routes the transmission to that channel. At the same time, it sends a signal back to the user's radio, which beeps to indicate that a channel has been located and is ready for the transmission. This entire process, in a well-designed system, takes place so quickly that it is nearly transparent to the user. When the user pushes his transmit button, the radio beeps, and the user can begin to talk.

Most of these trunked systems operate in the 800 MHz radio band, which is a fairly high frequency. The bands for public safety communications are Very High Frequency–Low Band (VHF-Lo), Very High Frequency–High Band (VHF-Hi), and Ultra High Frequency (UHF). The 800 MHz frequencies lie within the UHF band, which is more suitable for communication in urban environments than in rural areas.

Trunked radio systems have a number of advantages. The biggest advantage is that a relatively small number of channels can serve a large number of users. In a typical non-trunked system, a different channel is required for each operational unit or sub-unit. The law enforcement agency might need one or more channels for patrol operations, plus an auxiliary channel for running records checks and other less critical traffic, plus separate channels for specialized units and covert operations. The fire department requires one or more operations channels, and EMS needs their own, as well. Some of these channels might be silent much of the time (unless the fire department or EMS is constantly running calls), but they have to be kept in reserve because they could be needed at any moment. In a trunked system, it is only the number of *simultaneous* transmissions that is critical (the system can't carry more simultaneous conversations than it has channels).

Another advantage of a trunked system is that the system administrator can create an unlimited number of "talk groups." A "talk group" is the equivalent of a unit that would otherwise be given its own channel to use. When a user is assigned to a "talk group," he hears transmissions from other members of the talk group, and they can hear him, but he does not hear transmission from other talk groups. Users can change talk groups by switching a selector on their radio, similar to changing the channel on a conventional radio. The talk groups are created at the base station (although some users may be able to do this remotely from the field).

Each radio is identified by a digital code that is sent each time the transmit key is pressed. This digital code makes it possible to "lock out" a radio from the system if the radio is stolen or misplaced. The system administrator can tell the system to stop recognizing that radio's digital code, and the radio becomes incapable of sending or receiving traffic on that network. The radio can be re-enrolled in the system if it is later recovered.

Another advantage of the digital coding is that the source of every transmission is identified as soon as the transmit key is pressed. This can be important for a police officer or firefighter who is able to key his radio but unable to speak for some reason (such as being disabled or under duress). The identification of the transmitter is displayed on the dispatcher's monitor as the identifier sequence is received (if the communications center has this capability). From a management perspective, transmitter identification has the advantage of discouraging users from transmitting unauthorized traffic.

Some radio systems (not just those that are trunked) can be encrypted selectively. Certain transmitters can be set to digitally encrypt transmissions, which are decrypted when they arrive at an authorized receiver with the proper decryption keys. Listeners without the decryption keys hear only noise when they try to listen in. Encryption is useful for certain high-security operations, such as hostage crises and search warrant executions. With some systems, encryption decreases the range and clarity of transmission, so it is important to check with the radio manufacturer to see whether encryption will adversely impact the efficiency of your radio system.

Trunked radio systems can actually produce revenue. If the purchaser buys more channel capacity than is needed for its operations, then the owner can sell the surplus capacity to anyone in the operational zone. Thus, a county that purchases a trunked radio system with excess capacity can sell the extra capacity to local public works, public utilities, tow truck companies, ambulance services, or any other mobile radio user. The county maintains the network for its own operations, and the only extra cost is for the radios themselves, which would presumably be paid for by the users. Renegotiating the sale of extra capacity yearly allows the local government to re-assess its radio needs periodically to determine how much extra capacity it can sell. Sharing capacity in this way also allows the local government to communicate directly with other agencies in the event of a local emergency, by adding them to one or more public safety talk groups.

In trunked radio systems, the central station housing the computer that controls the system becomes a nerve center for all users. If this unit is destroyed, disabled, deprived of power, or otherwise compromised, the system becomes all but useless. Conventional radio systems can still (under some circumstances) communicate with one another to the limit of the range of their portable transmitters, but trunked systems are dependent on the network. It is vital that the facility that houses this resource be target-hardened, and provided with its own power supply, in case it should come under attack or be deprived of normal utility support.

Global Positioning Satellite Systems

Global positioning satellite (GPS) technology allows the user to establish, to a very high degree of accuracy, his or her location in three dimensions anywhere on or above the surface of the earth. GPS systems were extremely costly a few years ago, when the technology was new and development costs were being reclaimed. The newest GPS systems are not only far cheaper, but they are also smaller—a GPS receiver can be built into a wristwatch. These systems have a number of applications in public safety but they have some drawbacks as well—most of them based on the human factor.

The federal government has placed into orbit a constellation of 24 global positioning satellites. Their 11,000 mile-high orbits are coordinated so that at least five are visible from any point on the planet at any time. A GPS receiver needs to be able to "see" only four satellites to establish an accurate location. GPS works marginally, if at all, when there is no clear view of the sky above the receiver. Thus, GPS receivers do not work indoors, or where there is anything overhead more substantial than clouds.

GPS satellites are essentially highly accurate atomic clocks, mated with radio transmitters. Each satellite continuously broadcasts a unique digital signal to the earth's surface. The GPS receiver calculates

A countywide communications system

Washington County is one of three Oregon counties making up the Greater Portland Metropolitan area. The county seat, Hillsboro, is approximately 20 miles west of downtown Portland. The county covers 727 square miles, with a population of 404,750.

The Washington County Consolidated Communications Agency (WCCCA) provides all public safety communications for Washington County, Oregon. WCCCA serves 18 jurisdictions for 911 and dispatch services; 19 jurisdictions for computer-aided dispatch (CAD); and 25 departments or jurisdictions for 800 MHz radio or data services. Each city and fire district and the county are parties to an intergovernmental agreement for the entire county.

In 1991, WCCCA issued an RFP for an 800 MHz trunked simulcast communications system. The objective was to create interoperability throughout the county, regardless of jurisdiction or function. A $16.3 million levy approved by county voters paid for the new system, which was purchased from Motorola.

The operating costs of the system that was built are shared on a per device basis, and the per device cost drops as more devices are added. Therefore, WCCCA has welcomed opportunities to add users to the communications systems beyond traditional public safety agencies. For example, over the past four years, three separate public works departments were added to the system, as well as a sewer agency, the county's juvenile department, and a school district. As a result, the per-device cost has dropped from $183 to $112.

Adding non-public safety users has been a good idea for several reasons. First, most of their activity happens outside heavy dispatch peak times. For example, when the weather is bad, schools close. Second, having more eyes and ears connected to the county's public safety communications system is invaluable in times of crisis. If the sewer employees drive past an intersection on their way to check a plant and see that it is flooded, they can notify public safety or public works.

Another opportunity to reinforce the financial security of the system arose when neighboring Clackamas County began exploring ways of obtaining access to public safety data. Clackamas County had a technology grant but could not afford to install a communications backbone. Instead, in 1996 it installed WCCCA mobile data terminals in its police vehicles and built two mountaintop sites to provide microwave links to the WCCCA system. In 1999, a 10-year contract was signed by Clackamas County and the WCCCA to continue this successful business arrangement.

WCCCA is now investigating a partnership with a second county, and is implementing an upgrade to support this expansion. The new system, called SmartZone, adds digital capabilities and allows for communication between antennae at greater distances from one another.

WCCCA believes good business decisions are those that enhance the systems you have and increase interoperability among governmental agencies. Equally important is the ability to lower costs by sharing those costs among many users. While WCCCA has recognized the significant savings technology can provide in lieu of personnel costs, it has become increasingly clear that working across boundary lines for the sake of efficiency and cost effectiveness is another very good idea for everyone.

For information about this countywide system, visit http://www.teleport.com/~wccca or contact RoxAnn Brown, director, WCCCA, 503/690-4911, ext. 206; rbrown@wccca.com.

Questionnaire for evaluating public safety radio communications

It is very likely that many public safety agencies in your region are contemplating replacement of their radio communications systems. The following questionnaire is intended to help elected and appointed officials and policy makers understand the current condition of public safety wireless communications and interoperability within their jurisdiction, region, or state. These questions may also be useful in evaluating public safety communications systems funding and development proposals.

The number of major public safety incidents within the last year that required state and local public safety agencies to work together is ______.

The number of regional public safety employees has increased by _______ percent in the past five years.

The mission of public safety agencies in the region has changed in the following ways during the past five years:

The number of separate public safety wireless communications systems currently operating in the region is: (list individual agencies)

The public safety radio systems operating in the region are _____ years old.

The following mission-critical requirements are not currently met by the existing systems:

- coverage
- channel capacity
- interoperability with state agencies
- interoperability with local agencies
- interoperability with federal agencies
- data communications capabilities.

The following agencies are planning to upgrade or replace their systems in the next five years: (list individual agencies)

The replacement of these systems individually will cost approximately ______ million.

The amount of additional spectrum needed to support current and future public safety communications needs is _______________.

There (is/is not) _______ a person or office in the regional administration dedicated to public safety communications issues.

My jurisdiction, region, or state has established the following criteria to evaluate proposed radio system replacements: (list)

There (is/is not) _________ a funding source available or one that can be targeted for public safety wireless communications.

The region has explored the following federal initiatives supporting public safety communications for support and potential fiscal resources: (list)

Partnerships with the following local, regional, or state agencies have been explored for shared systems development: (list)

Source: Public Safety Wireless Network, "Public Safety Wireless Communications Systems—A Priority Investment for America's Future Safety," Program Information Brief, 1999.

its distance from each individual satellite and compares distances from different satellites against an almanac programmed into it that tells it where each satellite will be at any time. The receiver can establish its own location with an accuracy of a few meters. (An excellent online tutorial describing GPS technology is available at http://www.trimble.com/gps/index.htm.) In fact, advanced techniques allow a location to be established to within a few *centimeters*, but this kind of accuracy is usually unnecessary for public safety applications.

The most common use of GPS in public safety is to locate mobile assets from a central control station. A typical display map of a city's police, fire, and EMS resources defines areas of responsibility (zones, sectors, commands, precincts, etc.), and possibly the location of a station or substation in each area, but it doesn't tell the viewer where the mobile units assigned to those areas actually are. A unit may be at the station, away from the station on a call, or in another area for backup. Officers may report their location inaccurately or ambiguously, or not at all. When a quick response is required, or when a unit requests assistance without giving a location, a GPS system can be very useful.

A GPS system can also be useful in plotting maps of incident locations over time. The tools that are used for this kind of analysis are collectively called a geographic information system or GIS. GPS is usually, though not always, mated with GIS to produce the data, which can be used for everything from patrol officer deployment to the siting of utility stations. A number of firms produce mapping software keyed to GPS-generated coordinates, but these maps seldom reflect the actual geography of the area. A large building or complex, such as a hospital or high school, will probably show on the map as a small dot or single point, even though the facility covers many acres. Most of these software maps allow for the "drawing" of features on the map, but this can be a costly and time-consuming task.

To build an accurate local map, local jurisdictions can contract for a "flyover" of the city or county to create detailed aerial photographs. The photos are used to plot all structures and significant terrain features onto a map overlay, synchronized with latitude and longitude data. It is even possible to embed into these maps floor plans of buildings, so that fairly precise interior locations can be established on the map display. Tactical police and fire commanders find this kind of information extremely useful for planning and for incident management, but this level of detail is costly.

A GPS can be used to track the movements of a receiver, or the vehicle on which it is mounted. Because the GPS system updates the location of receivers up to several times a second, direction of travel and speed can be tracked with high accuracy, and either transmitted to a base station or stored for later retrieval. This kind of information can be used to verify the speed of fire apparatus or a law enforcement vehicle en route to an incident, if needed. It can also track the movement of the vehicle during a duty shift, to investigate allegations of malingering or misconduct.

> **It is even possible to embed into these maps floor plans of buildings, so that fairly precise interior locations can be established on the map display.**

This sort of "telltale" tracking is useful from a management standpoint, but public safety personnel often resent it and go to considerable lengths to thwart the system. Law enforcement officers, in particular, value the freedom to roam within their patrol areas and determine their own activities minute by minute. GPS monitoring can be perceived as oppressive and lead to conflicts with management. In an early GPS trial, one state patrol agency mounted GPS receivers in their patrol vehicles. The receivers transmitted the precise location of the vehicles whenever the officer keyed the radio transmitter, or on a command from the communications center. Officers referred to the system as "Sergeant Hiding In Trunk" (or more commonly by the acronym that label created), and sometimes parked under freeway overpasses to block the signal from the overhead satellites and momentarily disable the system.

The use of GPS technology has even found its way into some employee labor contracts. In some jurisdictions, a GPS location signal can only be broadcast from a patrol vehicle when the officer triggers it manually, or remotely only during a verified emergency.

Wireless Data and Laptop Strategies

The evolution of the two-way radio has probably had a greater impact on the way that public safety personnel work than any other technology. Useful as they are, traditional two-way radios transmit mainly voice traffic, and the communications operator is the critical link between the field officer and all of the resources that he or she may call on. While no wireless data solution can replace a good communications operator, two-way radios that can transmit data can greatly augment his capacities. The wireless system can connect the person in the field to the relevant database so that he or she can get information directly, instead of waiting for it to be read by a dispatcher. Bypassing the dispatcher makes for a more efficient field force, and encourages greater use of the information systems.

Most mobile data applications are designed for use in a car or truck, but there are now handheld palmtop computers and two-way pagers that bring mobile data capabilities to employees working from bicycles and motorcycles, on horseback, and even on foot.

When police, fire, or EMS personnel have an efficient mobile data system, information is sent to them as text, in the same form that the dispatcher sees. Frequently, emergency calls are still dispatched by voice, so that all units on the network are aware of the incident, but the same information is available on a mobile terminal in front of the field workers. Depending on the sophistication of the system, field workers may be able to bring up diagrams or maps of the area to which they are responding, research the system for previous calls to that area or address, and gather intelligence on the incident as they respond.

Law enforcement units make more use of these systems than do other public safety components, because they usually handle more and a greater variety of incidents than do fire and EMS personnel. In agencies where mobile data systems have been introduced, there is an almost universal trend: the rate of recovery of stolen cars increases, as does the numbers of arrests for outstanding warrants. When officers can make these inquiries quickly and easily, they make more of them.

> **Field workers may be able to bring up diagrams or maps of the area . . . and gather intelligence on the incident as they respond.**

There is also a common downside to installation of MDTs in vehicles, particularly in police vehicles: accidents involving patrol cars tend to increase. Every MDT manufacturer and local government agency that uses MDTs has a policy that warns the operator of the vehicle not to use the MDT while the vehicle is in motion. Unfortunately, when officers know they have information at their fingertips, they want to use it as much as possible, and they don't want to pull to the side of the road to do it.

A voice interface option for the MDT may reduce this problem, if not eliminate it. One vendor now offers a voice recognition interface that allows a mobile operator to make inquiries and receive replies to those inquires without taking his or her eyes from the road. The voice interface system works with most of the wireless data equipment marketed to public safety.

Mobile data terminals. There are two types of MDTs mounted in vehicles:

- "Dumb terminals," capable of interacting with the wireless network, sending and receiving messages, and performing common dispatch functions
- Laptop computers that incorporate all the capabilities of the "dumb terminal," but add the flexibility of a computer to run word processing, database, mapping, and other software.

When laptops were a lot bigger, more expensive, and fragile, the "dumb terminal" solution was by far the most popular. However, now that laptop computers have evolved and decreased in price, far more agencies use laptops, or some other configuration of a full-fledged computer, as the hardware platform for a wireless data system.

Some companies have developed fully capable "laptop" computers especially for use in mobile environments. The word "laptop" is in quotes here because these machines would be very difficult to use on one's lap. The display, keyboard/input device, and central processing units (CPU) are all mounted separately. These hardware designs are more expensive than an off-the-shelf laptop, and generally they can't be taken out of the car for use elsewhere. However, they give more flexibility with regard to mounting in the car, and they tend to be more durable.

The mounting of equipment in emergency vehicles has become an important issue as passenger compartments have gotten smaller, and equipment has to be kept clear of the deployment zone of the car's air bags. Radios, siren and emergency light control panels, radar units, mobile video recorders, mobile data terminals, and rifle/shotgun racks all compete for space with the driver and passenger.

Laptop displays aren't generally intended to be used in mobile environments, and it shows. In the daytime, they are often too dim to be read clearly in direct sunlight, and at night, their glare may impair the driver's night vision. The screen brightness of some modular displays, like those described above, is adjustable over a wide range, so that they can be read during the day or at night without strain.

Many of these displays are also touchscreen-sensitive, so that the operator can click buttons and make short text entries without using a keyboard. This is often useful for pre-programmed functions, such as advising of arrival at an incident, signaling a traffic stop, or calling for help in an emergency. When the operator needs to make a more complex text entry, he can use a conventional keyboard, which might be stowed beneath other equipment on the floor, or in some other less obtrusive location.

> **Laptops are most often damaged when they are taken out of the car.**

When buying conventional laptop computers for use as mobile data hardware, a public safety agency generally has two choices. The agency can buy laptop computers of normal durability, and purchase extra, to be used as replacement units when the primary units are damaged or lost; or it can buy "ruggedized" laptops, which are more durable and will not need replacement as often. The second choice usually in cludes some wishful thinking. Even though some ruggedized laptops can withstand being run over by a large truck, they will still break down, sooner or later, and will have to be replaced.

Ruggedized laptops are heavily cushioned against shock, sealed against water and dust at every possible entry point, and insulated to be able to operate in temperature extremes. Some of them will continue to function while immersed in water. They are generally heavier than standard models, slightly bulkier, and cost approximately 50 percent more than a non-ruggedized computer of comparable specifications.

Experience has shown that laptops are most often damaged when they are taken out of the car. For example, agencies that issue laptop computers to employees at the beginning of each duty shift, intending that the employee should mount the laptop in the vehicle and then return it at the end of the day, find that the machines get left on the hoods of cars, fall off their mounts, and suffer other, similar abuse. Even when the laptop is in the car, it is subject to Gagne's First Law (named for Alec Gagne, a Morgan Hill, California, police officer): Any horizontal surface in an emergency vehicle, no matter how costly or delicate, will be used as a coffee cup holder.

Whatever strategy you choose, make sure that you have enough replacement units on the shelf to issue when primary units go down, as they inevitably will. To make the laptops last as long as possible, minimize the number of times that they are removed from their car mounts, through a combination of wise equipment purchasing, good training, and judicious policy formation and implementation.

Network infrastructure. A wireless data system requires a fairly complex network infrastructure. A server capable of interfacing with the local computer-assisted dispatch (CAD) system and with the wireless "backbone" has to be in place, and the software on board the mobile units has to be compatible with that server and with the databases that it will be accessing.

There is also an issue with how the data will be transmitted. For many years, in order to have a wireless data network, the user also needed to have access to one or more dedicated radio channels to carry the data. As discussed previously, these radio channels are increasingly difficult to obtain, as bandwidth becomes more precious. Further, many local governments provide services to areas where there is little or no radio coverage.

Fortunately, cellular telephone networks can be used for public safety data communications, and provide good security and relatively low cost. Even where a public safety radio network has dead areas, cellular phone users can still communicate in all but the most remote areas. The explosion of the cellular telephone industry has provided the necessary capital to erect cellular towers sufficient to ensure that cellular customers are very seldom out of touch.

The technology that makes cellular telecommunication possible is called CDPD–cellular digital packet data. With CDPD, data are moved through the network in a way very similar to the way that electronic mail and other data are moved through the Internet. CDPD uses a similar scheme, but instead of transmitting information over a hardwired network, the packets are converted into digital form and then sent over the cellular bands (radio channels designated for cellular traffic by the Federal Communications Commission). Depending on the system in use, they can be sent over cellular channels not in use at that moment, or interspersed with other regular cellular traffic. As long as the user is within range of a cellular relay tower, the message has a high likelihood of getting through intact. Approximately 85 percent of the geographic area of the United States, and 99 percent of the population, has cellular coverage.[2]

The advent of CDPD places the capability of a wireless network within the reach of most local governments, regardless of size. Before CDPD, an organization that wanted wireless data communications had to have the capital to build its own wireless infrastructure, with relay stations, repeaters, and reserved radio channels, all of which was prohibitively expensive for all but the largest local governments. CDPD eliminates the cost of having to build that infrastructure, as it is already in place. A public safety agency can also create a hybrid network, sending data over a cellular network where that network is available, and over a conventional radio channel where it is not.

CDPD places the capability of a wireless network within the reach of most local governments.

One vendor is offering a turnkey MDT system that is based entirely on CDPD. For approximately $300 per month per terminal, the vendor provides all of the hardware, software, and support necessary to establish wireless data capabilities. This might seem to be a steep cost, but when one considers the cost of purchasing, configuring, and maintaining servers, software, data connections, and the other infrastructure associated with this project, $300 per month can be a real bargain.

Gauging effectiveness. To measure the potential effectiveness of a wireless data system, a task analysis may be necessary. How much time is spent at headquarters, completing tasks that could be accomplished in the field with a wireless system? How many inquiries of databases are not made because the police officer in the field doesn't want to take up valuable airtime, or can't get on the air because of other traffic? Will the information supplied by a wire less system allow your employees to complete all of their administrative tasks in the field? If there is even one item of information that can't be obtained in the field, or one task that can't be performed to complete a process, then the trip to the station will have to be made, anyway.

Organizational impact. Introduction of wireless systems may require some re-education and organizational change in order to make them effective. Public safety workers, like those in other industries, use the office or station as a social center, as well as a workplace. Employees return to headquarters to turn in reports and complete paperwork, and at the same time, socialize, catch up on internal goings-on, use the restroom, and perform other tasks, work-related and otherwise. Even if employees can perform all work-related tasks in the field, they will still want to return to the home base. Although telecommuting is a popular option among many employees, they report that they miss out on a lot of the informal communication that takes place in the office. The same thing is likely to happen when wireless data systems allow public safety tasks to be completed in the field.

Cellular Telephone Applications

Cellular telephones are now so commonplace and relatively inexpensive that many families have one for every member. Cellular telephone technology can be used to augment the capacity of public safety workers, but only with clear policies on use.

Any public safety worker may be called to duty at any time to respond to a local emergency. The smaller the community, the more likely this is to happen, as the available pool of personnel from which to draw is small in small communities. Pager systems can be used for one-way communication, but some public safety workers may also need to initiate communication from the field. Firefighters and EMS personnel often intervene in accidents and other unplanned happenings, and they may need a way to communicate quickly with their home base and summon additional help. How likely this is to happen depends largely on the makeup of the work force and your policies regarding off-duty responses.

Law enforcement officers are even more at risk for off-duty encounters, because many law enforcement officers routinely carry their badges, identification cards, and weapons while off duty. If they elect to intervene in a crime that they observe while off duty, their options, absent a reliable means of communication with the dispatch center, are extremely limited. If they decide to act in a law enforcement capacity, the fact that the firearm is one of their few decisive force options may cause them to escalate a situation beyond what would be required if they had all of the tools (including access to backup officers) normally available to them while on duty.

Some law enforcement agencies issue every officer a portable radio that he or she can carry while off duty. While this is certainly desirable, it is an imperfect option. First, even modern portable radios are bulky and uncomfortable to carry while in street clothes. Second, their range is limited, and outside of the jurisdiction where the officer works, they are useless, being beyond the reach of a base station on their frequency. Finally, if the officer needs to communicate with someone other than the base station dispatcher or another mobile unit (for example, a translator), messages must be relayed through the dispatcher, which is inefficient and inconvenient.

Deploying cellular phones to employees on a wholesale basis can invite misuse and public criticism. If employees are not required to account for use of cellular airtime, they will quickly come to regard it as essentially free and use it indiscriminately. The key is to arrive at a method and policy that permits and encourages use of cellular phones for legitimate business, but makes the employee personally accountable for all other charges associated with the cell phone.

> **The objective is to provide the employee in the field with as many communications options as possible.**

Cellular airtime bills generally account for every call, providing both the duration of the call and the number of the telephone on the other end of the call. The cellular service provider can often customize billing to meet the needs of the local government that needs this level of accounting. Bills can be supplied in computer-readable form, and calls made and received can be cross-indexed with indexes of telephone directories. Management services will perform this kind of analysis for a nominal fee, which is quickly recovered through the elimination of unnecessary calls made at public expense. Employees can be required to keep a log of calls made and received, and to reimburse the city or county for any calls that are unrelated to official business. Just knowing that their call activity is being continuously monitored will keep many employees from using the phone for personal or otherwise unnecessary calls.

Another option might be to allow employees to obtain cellular service at the local government rate, which is often substantially cheaper than any available to a business or individual user. The employee pays the monthly service fee and for any airtime usage that is not attributable to official business. In the alternative, the employer could pay the monthly service fee, to overcome any resistance from individual employees who don't want to make a personal investment in cellular service. This gives the employee the benefit of having a cellular phone to use for any purpose and gives the employer the benefit of having employees reachable by cell phone.

Many cellular phones can be configured to make and receive calls from only certain predesignated numbers, including 911, or some other programmed emergency number. Some law enforcement agencies give programmed phones to the victims of domestic violence and stalking. The phones can be used only to summon help in an emergency, and thus have a low potential for abuse.

Whatever cellular telephone strategy you elect to use, remember that the objective is to provide the employee in the field with as many communications options as possible, so that they are not committed to a single, undesirable course of action in an emergency.

Digital Record-Keeping Systems

Most of the records that local governments create are still on paper. Managing all of that paper is an expensive and perilous process. Digital imaging systems allow paper records to be archived with built-in redundancy in the form of backup copies, and can provide almost instant access to any record via a properly networked system. Scanned copies of paper records can be interleaved and integrated with records that start out in digital form, such as dispatch logs, voice recordings, and digital images.

Most of these records are stored on digital media, such as CD-ROMs, which hold about 650 MB of data per disk. Not long ago, machines to create CD-ROMs from blank disks cost $10,000 or more. Today, they can be had for less than $200, and the blank disks cost about a dollar a piece in bulk. Users can archive their data inexpensively to a medium that is very easy to access and make cheap redundant copies for remote storage, to ensure that no single disaster or theft can destroy the data. Because the shelf life of recordable CD-ROMs is relatively short (perhaps only ten years), a public agency must put in place a long-term plan for upgrade and maintenance if it chooses this medium for permanent storage.

At this writing, the equipment to create the much higher density DVD disks is still expensive, but prices for this equipment are likely to fall within a few years. This will allow storage of as much as 24 times as much data on a single disk as is allowed by CD-ROM technology.

CD-ROMs are typically stored in a “jukebox” that allows disks to be shuffled in and out of a CD-ROM drive as needed. The number of disks that can be accessed at one time is determined by the number of active drives, and the storage capacity of the jukebox varies with the model. These systems are fairly large investments initially, but they can save a great deal of money in the long run, supplanting the need to store paper records, magnetic tapes, and other records, while at the same time ensuring that the information will remain available. Magnetic storage media, such as floppy disks, hard drives, and recording tapes, can be erased with a strong magnetic field or electronic pulse, and are thus fairly fragile. Plastic CD-ROMs are not affected by magnetic fields, and remain readable unless severely defaced or broken into pieces. It would be difficult to accidentally destroy an archive on a CD-ROM disk.

The transition from a paper to a digital archiving system is expensive. Each paper document must be scanned into digital form. Companies such as Xerox and Bell and Howell sell equipment and services to expedite this process, and service companies will contract to scan documents. Only after the archiving process has been checked for completeness should the original records be destroyed.

Intelligence Analysis and Expert System Software

Law enforcement investigators often have too much rather than too little information, and must manage the information and make sense of it. For example, leads are often generated by a pen register, a device (more commonly now, a software program) that records the numbers dialed from a telephone where the register is installed. Digital switches and other innovations of the telephone industry have made it possible to capture the numbers of callers to that telephone, as well.

The investigator using this information is confronted with long lists of telephone numbers, with time and duration of calls, and possibly gets the names of the persons or companies who subscribe to those phone numbers. With this information, the investigator can find out who is in communication with the suspect, and what relationship the suspect might have with each person or entity. In many cases, the majority of the calls are either legitimate or inconsequential and have no impact on the investigation. Of course, the trick is to figure out which calls are important to the investigation.

> **Data mining involves searching huge repositories of information for records relevant to an investigation.**

Narcotics, fraud, and vice investigations most often need to track calls, and they also tend to involve large numbers of people, both suspects and victims. The classic analysis technique for this type of data is the link chart. Each person, place, call, and/or event is written on a card, and the card is posted on a bulletin board. Lines are drawn between card(s) that involve the same communication or transaction. The center of the activity is usually found where the lines begin to converge.

As the number of people, calls, meetings, and transactions increases, a bulletin board is inadequate. However, intelligence analysis software can easily keep track of all of the relationships in an investigation of this type, and display them in any number of ways. By accessing other databases and comparing the information contained in them against that in the intelligence database, the investigator can associate persons with businesses, vehicles, telephone numbers, bank accounts, real estate and other items that may be fruits of a crime, or leads to other elements in the enterprise.

A data mining utility or service is often used with intelligence analysis software. Lexis-Nexis and DBT Online are the two largest providers of this service to law enforcement. In this context, data mining involves searching huge repositories of information for records relevant to an investigation. Law enforcement databases can be searched, as well as records maintained by the private sector, or records databases from non-law enforcement governmental sources. These records can include credit histories, records from licensure bureaus (professional licenses, concealed weapons permits, disciplinary records), tax assessor records, telephone numbers, city directories, and so on. Online searches can be done cheaply and quickly, and they retrieve information that used to require weeks of sifting manually through courthouse records to find. As with pen register records, these searches can yield an over

Sharing public safety records

In July 1998 law enforcement representatives from several south-central Minnesota counties and cities began a collaborative effort to share records and equipment and to control costs. Representatives from five counties and sixteen communities attended a meeting to discuss common concerns and opportunities:

- Present systems were at least 10 years old; most did not capture information for analysis of crime trends.
- Most databases were proprietary; information could not be easily formatted to allow sharing with other systems.
- Modern dispatching requires fully functional, computer-assisted dispatch (CAD) systems—something no agency was using.
- The participating communities needed to improve their ability to recover from natural or human-made disasters.
- Public safety officials were frustrated by their inability to share information about persons and crimes with other agencies.
- Deputies and officers needed to be out in the community and on the streets, rather than in the office.
- Information from the very small police departments should be available at a reasonable cost.
- Courts, corrections, and human services should be able to integrate systems to allow seamless tracking from point of contact through sentencing and probation.
- A shared system should not preclude local control of creation, modification, deletion, and/or dissemination of sensitive files.

The group discussed whether a system could be designed and implemented that solved all or most of these issues while also linking together the many agencies. Such a project would obviously present technical challenges. But the real hurdles would be changing the traditionally protective culture of many law enforcement agencies, and educating elected officials about the viability and benefits of a fully-shared records system.

As discussions progressed, the participating sheriffs and police chiefs set aside any reservations they held about developing a shared records system and decided they needed a strategy that would develop a "big picture." This strategy would consist of information that could be analyzed to study crime trends and assess the most effective responses—starting at the time of roll call, crime detection, reporting and arrest, and concluding with sentencing and probation.

The integrated system was designed around enhanced computer-aided dispatching (CAD), an advanced records management system (RMS), and a mobile digital computing (MDC) system. Other programs included in the system include jail records management, civil process, and photo imaging.

The city of Mankato and Blue Earth County had recently formed the Joint Services Bureau, a joint powers entity, to oversee initiatives shared between the two agencies. (Joint Services presently encompasses dispatch operations, records functions, issuance of permits, and tobacco retailer licensing.) Mankato Deputy Director Jerry Huettl, who serves as administrator of the Joint Services Bureau, was asked to oversee researching the many questions associated with a shared records system. Over the next few months, the effort included evaluating vendors, preparing budgets, holding meetings with elected officials, and presenting information to the various partners.

After a review of many possible venders, the group chose Computer Information Systems (CIS) for two major reasons. First, eighteen counties in the state currently use the CIS system. Additionally, the Minnesota County Computer Cooperative (MCCC) recognized CIS as an approved vendor for this type of records system. The system was implemented in late December 1999. The leaders of the effort to share public safety records management in south-central Minnesota believe that the single most important element of success has been the cooperation and buy-in of agency leaders and elected officials.

Source: Based on an article by James Franklin and Jerry Huettl titled "Sharing Records," which appeared in the November 1999 issue of *Minnesota Cities* magazine, a publication of the League of Minnesota Cities.

whelming amount of information, but when used in conjunction with intelligence analysis software, the information can be managed and the relationships between subjects of interest can be made more apparent.

A homicide investigation can involve hundreds or thousands of interviews, each of them containing information about cars, people, animals, times, dates, and places. Some intelligence analysis packages can "mine" narrative reports for this information and catalog it into the database. As a result, the chance that a lead or relationship will go unnoticed is greatly reduced, and a much greater percentage of cases are solved and closed.

Expert system software uses a technique that is similar, in that it brings to bear the skills of experienced investigators to analyze information. To create an expert system, the developer brings together people with substantial experience in the field and asks them to articulate the rules that they use to reach conclusions. Many experts aren't aware that they use rules, as they often work intuitively, rather than deductively. By asking, "How do you know this?" the developer establishes the methods by which they reason, and the assumptions they make.

The developer of an expert system incorporates thousands of these methods and assumptions into a matrix. Improving the matrix tends to be a never-ending project, as methods and situations change over time, and the confidence level of each assumption is likely to change. The best expert systems refine their own values, based on verification of accurate conclusions.

The investigator using an expert system fills out a questionnaire that captures relevant data from each case to be analyzed. Once the data are captured, the expert system can produce a list of assumptions about the suspect(s), each with an assigned confidence level. The result is essentially a profile of the most likely suspect(s) in this case. The result provides the investigator with leads that he might not be able to derive on his own. A system like the one described here, targeted at career burglars, was instrumental in reducing residential burglaries by 32 percent over one year in Ottawa, Ontario.[3]

An expert system helps preserve the corporate memory in criminal investigations. The combined knowledge and experience of the members of an organization constitute its corporate memory. As investigators are transferred, rotated, or promoted out of their assignments, taking with them the experience that they gained in those positions, the expert system allows much of their expertise (and that of other agencies) to be archived and used in the solution of crimes that take place after the investigators who created the system are gone.

Expert systems are available for several types of criminal investigations, and others have been devised to predict police officer behavior and misconduct. Some systems work better than others, and each has to be carefully evaluated before purchase, because these systems tend to be very expensive. The software manufacturer has to invest thousands of hours of research before it has a product to market, and the customer base is comparatively small. When expert systems work, they can save many times their cost in losses that are avoided and manpower that doesn't have to be deployed.

Both intelligence analysis and expert systems software require that their users have a certain amount of expertise to use them effectively. The companies that make these systems always offer training in the use of the software, and many sponsor a user's group with periodic meetings. It is important that the people who will be using the software complete this training and stay current by attending the user's group meetings.

It is not uncommon for the chief executive or a senior manager from the agency making the purchase to reserve a training "seat" for him or herself, but unless the manager is going to be actually using the system, this is a waste of resources. More than one user should be trained, so that at least one is always available, but the manager who takes the training and then does not use it regularly will not maintain his or her skills. See that the training is given to the people who will make the greatest use of it.

Electronic and Voice Mail Applications

Because public safety is a 24-hour-a-day function, public safety employees' schedules are often not in concert with normal business hours. Employees have to be rousted from much-needed sleep to answer questions about operations from the previous duty tour, and meetings are difficult to arrange without paying overtime and disrupting everyone's schedule. Electronic and voice mail can be practical and relatively inexpensive solutions.

Electronic mail. E-mail can be used to disseminate information that would normally be reserved for real-time meetings. Face-to-face meetings have the advantage of being more conducive to discussion, and some topics should be reserved for these, because discussion can be a critical component of the communication for both management and labor. However, many routine communications can be sent by e-mail, saving valuable personnel time on both sides of the management-labor fence.

Internal e-mail is a resource that has to be used judiciously. It is very easy to get carried away with the ability to transmit information to every member of your workforce at one time and saturate them with too much data. If the message isn't important enough to announce at an "all hands" meeting, it probably shouldn't go onto the e-mail system.

Making your e-mail system accessible from computers outside of the office is often convenient, be cause employees can check e-mail from their homes while off duty, or from a hotel while on a vacation or business trip. However, this also opens a potential point of entry to vandals or hackers/crackers who may do damage to your network. If remote access is provided, it is critical that user names and passwords be kept absolutely confidential and changed frequently, and system administrators have to be especially vigilant. Unless there is a clear need to provide remote access, it may be preferable to restrict access to internal users only, or to forward e-mail messages to a personal account temporarily when an employee is going to be away from the office for an extended period.

If your e-mail system is configured to provide some or all employees with an e-mail account accessible from the Internet (e.g., name@anycity.ci.xx.us), then it is wise to put in place some well-defined policies on how employees are to use this resource. As citizens gain access to the Internet and get used to using e-mail as a routine and convenient form of communication, they will begin sending direct questions and comments to government employees, including public safety employees. Internet-based e-mail also provides a conduit for employees to network with their colleagues in other agencies and find new ways to solve problems and access resources. Employees can subscribe to professionally oriented mailing lists and participate in online discussions during business hours. These, among other things, are the positive uses of electronic mail.

> **Employees can have little expectation of privacy on a computer network.**

On the negative side, the Internet overflows with amusing but time-wasting features that can eat away at employee efficiency. Joke lists, personal correspondence, commercial solicitations (a significant fraction of which are of a sexual or pornographic nature), hobby-oriented mailing lists, and other non-business activities have no place on the local government network. If the media discovers these activities, they usually prove embarrassing for the employees that use the network. When employees use the network for recreational purposes, it also increases dramatically the likelihood that a computer virus will be introduced into the system, threatening all the data on the network.

Statutory and case law is clear: employees can have little expectation of privacy on a computer network, especially if the employer gives notice that activities conducted over the network will be monitored. It is important to make this policy known to all employees who use the network, and to follow up by randomly inspecting network files and e-mail folders to ensure compliance.

When relatively harmless unauthorized activity (such as personal correspondence with trivial content) is found, a personal word to the employee is usually enough to halt the activity. Word of this kind of monitoring travels fast through the informal network, and it will quickly become clear that "big brother is watching." Employees who wish to explore the Internet for personal activities should be encouraged to obtain their own e-mail accounts and do this on their own time. Those who can't afford computers of their own can usually find Internet access at a local school, college, or library.

Voice mail. Voice mail systems are especially valuable for public safety operations because employees work round-the-clock shifts and are frequently unavailable during normal business hours. When managers, other employees, and citizens need to contact these employees, they are often sleeping or pursuing personal activities. Electronic mail is an imperfect solution to this problem, because e-mail requires access to a computer on both ends of the communication, and that is not always convenient. However, most people do have access to a telephone. Written phone messages are less reliable especially because law enforcement employees, in particular, may be in contact with citizens who do not wish their names to appear on a message slip where it can be read by anyone who happens to find it.

With any type of public safety switchboard, message center, or headquarters, there should always be ready access to a human operator. Even though there may be an emergency number (such as 911) designated for emergencies, people frequently call non-emergency numbers with a request for immediate assistance. "Please hang up and call ____" is a highly unsatisfactory response in this situation. One of the first options callers hear, if not the very first, should be information on what key to push to immediately transfer to an emergency operator.

Most voice mail systems then allow the caller to hear the employee's voice speaking his or her name, followed by the mailbox number. If possible, key voice mailbox numbers to a number associated with the employee, such as a badge, commission, or payroll number, and put it on the employee's business card.

Employees should be encouraged, if not required, to update their greetings to reflect current assignments, vacations, or other circumstances that might affect when their voice mail message will be retrieved and answered. For example,

> "This is Paramedic John Smith, assigned to Anytown Fire Rescue Station Number Six during July. I will be attending in-service training out of town during the second week of July, and will retrieve my messages when I return."

This message alerts callers with an urgent need that they need to direct their request elsewhere. Because some employees may decide to get creative with their outgoing messages (usually not a good thing), supervisors should periodically monitor to ensure compliance with voice mail procedures.

Some voice mail systems allow an "urgent" code to be attached to a message. The "urgent" code has the effect of moving the message to the top of the message queue when messages are replayed, and can also cause an alert to be sent to the employee's pager or other alerting device. It is usually best to keep this option available for internal use only. Citizens may regard their request as urgent enough to disturb the employee while he is off duty, when this decision is better left to an on-duty supervisor. As noted above, if the message is more urgent, the caller should be directed to a human operator, who can either contact the employee personally, or refer the problem to someone who is on duty and able to respond to the problem.

Employees should be able to retrieve messages from any remote telephone. The retrieval access number and retrieval codes should be held as confidential, and employees should be required to change their passwords frequently to avoid someone "hacking" the voice mail system. To ensure that employees are monitoring and responding to voice mail, it may be wise for supervisors to leave messages from time to time. Most systems allow authorized users to leave a message in multiple voice mail boxes with a single call.

Voice mail is another form of asynchronous communication that can be very useful and user-friendly, if not misused. As with other systems, it requires that supervisors check for compliance with use guidelines from time to time to ensure that the "face" your agency shows to the public via its voice mail system is a professional one.

For more information on radio communications interoperability

Public safety work requires effective coordination, communication, and sharing of information between numerous criminal justice and public safety agencies. However, many radio communications systems currently in use are technologically obsolete and don't have the capacity to serve their community properly. In many communities, police officers, firefighters, and emergency medical service personnel responding to the same incident cannot communicate with one another.

Recent high-profile public safety incidents have focused attention on the critical role of public safety communications and the deficiencies of existing systems. But improving public safety communications is a complex undertaking. Local agencies will need funding, they will need access to the radio spectrum, they will need systems that can interoperate with those of neighboring jurisdictions and cooperating agencies, and they will need to be able to protect their new systems against security threats.

To address these problems, the National Institute of Justice (NIJ) has created a comprehensive program known as AGILE to pursue research, promote standards for public safety communications systems, evaluate systems, and provide information and assistance to elected and appointed officials to help promote informed decision making regarding issues of communications interoperability. For information about the AGILE program and its free services, contact Mike McGee, AGILE Education Programs Director, 800/416-8086 or mmcgee@du.edu.

[1] William Glanz, "Imaging Firm Battles Paper," *Baltimore Business Journal* 16, 10 (July 10, 1998).

[2] Cellular Telephone Industry Association, June 1999.

[3] *The Gazette*, Royal Canadian Mounted Police (February 1998), p.3.

Information and Communications
Technology for Public Safety

Volume 32 / Number 1
January 2000