Making Electronic Supervision Work

Technological innovations have changed the way many professions gather, store, understand, and disseminate information. Today, some of these same technologies are being used by correctional agencies to keep a watchful eye on offenders 24 hours a day, 7 days a week.

Although systems may differ, electronic monitoring is essentially a method of supervising offenders remotely. With an electronic monitoring system in place, probation and parole officers can track offenders whose movements and schedules are restricted (usually by the court) to approved places and activities. In addition to verifying the daily routine of offenders and confirming their adherence to imposed restrictions, some electronic monitoring systems can administer random alcohol and drug tests to check other court-imposed conditions.

Electronic supervision can be flexible and used in many ways, such as to enhance public safety, promote the safety of individual victims, hold offenders accountable, foster behavior change by offenders, reduce jail or prison populations, and provide correctional services economically. But technology is only a tool.

(See Electronic Supervision, page 3)

Fall 2002

IBETing on a Secure Border

The almost 4,000-mile-long border between the United States and Canada is the longest undefended border in the world. But this boundary line has been changing—from one that is open and safe to one that requires increased security and policing, especially in light of last year’s terrorist attacks and the 1999 arrest of an Algerian national in possession of high explosives.

Even before September 11, 2001, illegal trafficking in contraband and humans had drawn the attention of law enforcement agencies on both sides of the border that had to consider that trade between the United States and Canada is among the most vigorous in the world—more than $1 billion a day. Slowing this activity to a more secure crawl could create economic risks for both countries. The border—on land, on the water, in the air—must be open but closed to crime.

In 1996, the United States and Canada formed the first Integrated Border Enforcement Team (IBET) to combat smuggling and illegal immigration on the northwest border between Blaine, Washington, and British Columbia. Since its initiation, the West Coast IBET has seized an average of $1 million per month in drugs, weapons, alcohol, tobacco, and vehicles. Its success led to the formation of the Central St. Lawrence Valley team in the Cornwall, Ontario/Massena, New York area and to the ongoing development of four more IBETs.

IBETs draw together the full range of law enforcement resources, including small municipal police departments and tribal police; State and Provincial police and law enforcement agencies; the U.S. Customs Service; the U.S. Border Patrol; the Bureau of Alcohol, Tobacco and Firearms; the Federal Bureau of Investigation (FBI); the U.S. Secret Service; the Royal Canadian Mounted Police (RCMP); and the Canadian Immigration and Refugee Protection Service. The most recently established team is in Detroit, Michigan/Windsor, Ontario area. This IBET has 12 core agencies and 25 affiliated agencies, ranging from the Amberstville Police Service to the Consul General of Canada and the FBI.

“The cooperation that is the basic for this [IBET] has existed for many years,” says Peter Laun, Law Enforcement Coordinator for the U.S. Attorney’s Office for the Northern District of New York. “Bringing together an IBET in a particular location formalizes a long-standing informal, but effective, law enforcement relationship. The IBET forges a better understanding of the relationships between agencies and planning for larger scale operations, not just joint patrols.”

In early October 2001, the Cornwall/Massena IBET organized a large-scale, 2-day exercise involving approximately a dozen law enforcement agencies from the United States and Canada. During the exercise, Laun says, participants immediately recognized that communications deficits hampered the operation. Even though participants had created common maps and grid systems to locate the patrol boats, they still had trouble telling them apart. Participants realized they needed a way to plot, locate, and identify the boats from the air or ground.

Following the exercise, representatives from all the U.S. and Canadian agencies and the U.S. Border Patrol office in Massena met to discuss how technology could help make operations safer and more efficient. Working groups were established to deal with such issues as radio interoperability and vehicle-stopping technology. The National Institute of Justice’s National Law Enforcement and Corrections Technology Center (NLECTC) system joined this effort at Laun’s request.

Creating a “Smart” Border

Since September 11, IBETs have acquired sensor systems, night-vision devices, computers, global positioning systems, and automatic personnel and vehicle locators. But integrating advanced technology into IBET tactical operations is proving to be a challenge. Most IBET participants are law enforcement managers and agents, not engineers. For help in procuring and applying technology to create a “smart” border, IBETs have turned to NLECTC–Northeast and the Border Research and Technology Center (BRTC). “This was not a theoretical situation,” Laun says. “We found we really needed assistance to do it safely and efficiently. We needed the manpower multiplier of technology.”

Through BRTC and NLECTC–Northeast, each IBET has access to the expertise

(See IBETing, page 2)
necessary to identify current and emerging technologies for border security applications in such areas as sensors and surveillance, intrusion and human presence detection, geographic information systems (GIS) and related crime-mapping technologies, tracking, criminal information sharing systems, and less-than-lethal technologies designed to stop boats and other vehicles.

Ground sensors are among the technologies being explored. "Machines don't get tired like humans do," says Gordon Dilmore, a law enforcement specialist at BTCT. The Border Patrol began using ground sensors in the 1960s by adapting sensors originally designed to locate prospective energy deposits for the petroleum industry. After the Vietnam War, the Border Patrol, in cooperation with RCMP, started utilizing such systems. But these systems were vulnerable to false alarms from natural or legitimate causes.

Most current ground sensor systems provide only an "event cue." However, some promising experimental sensors provide video or audio cues. According to Dilmore, a Samila National Laboratories and Eastern Kentucky University project involves linking seismic sensors with a laptop computer and a video camera. The unit is connected to a real-time telephone to provide a real-time image.

In addition, closed-circuit television and microwave systems have been used by the Border Patrol in Vermont and New York State since 1984. "We will be looking at developing more of this technology for the IBETs," Dilmore says.

Crossing the Communications Border

The most challenging technology issue confronting IBETs is the need for communications interoperability. "You've got a lot of people involved and a lot of different communications systems, and they don't easily talk to each other," Dilmore says. "It's almost an overwhelming problem and there's been a rush to reach some solutions [since September 11]." The Cornwall/Massena IBET, he says, is currently sorting through many "perceived requirements" that are inevitable when so many agencies and groups are involved in such a large and complex undertaking.

One promising solution may be the ACU–1000 integrated switch, which handles virtually all of radio transmission systems. "The neat thing is that it will work with any of the existing communications systems, including cell phones, and will actually accept a phone call from the regular telephone system," Dilmore says. But the cost of developing such a system with its disparate pieces—managing for an urban center such as Washington, D.C.—can be prohibitive for the small rural operations common to the northern border. "Less elaborate and less expensive systems may ultimately offer more of a solution than systems that have all the bells and whistles," he says.

Another interoperability problem being addressed is RCMP's requirement for end-to-end encryption. End-to-end encryption means that on a message (either voice or data) is encrypted on the other end of the communications circuit or path, that encryption remains intact until the message is received at the other end, even if the transmission protocol changes from analog to digital (or vice versa) or the mode of transmission changes from line to radio frequency (or vice versa). Although the ACU–1000 can handle end-to-end encryption, Dilmore says, many agencies do not have encryption capabilities. Existing links with RCMP may help solve this problem, but as long as the requirement for end-to-end encryption remains, some operations may be left out.

Besides the lack of radio interoperability, IBETs face the difficulty of reconciling different mapping standards: U.S. maps are in miles; Canadian maps are in kilometers. The solution for both sides may lie in military-style mapping based on integrated GIS technology.

Lessons and Technologies From the Military

Laun also cites the need for what the military calls "command and control." "What law enforcement along the border needs to have today," he says, "is more of a military capacity for joint command."

Dilmore, who worked in the Federal counterdrug program before retiring from the Border Patrol, says the IBETs need what the military calls C4ISR—command, control, communications, computers, intelligence, surveillance, and reconnaissance. To explain C4ISR, one must jumble the acronym a little: computers bring together the elements of intelligence about the adversary, surveillance of the area, and reconnaissance as to the adversary's current activities. Bringing this intelligence together in a digitized format facilitates communications between commanders and agents (command) and, thereby, control of the situation. This military analogy applies to IBET tactical operations: Keeping track of many disparate units is as real a problem in law enforcement operations as it is on the battlefield, he says.

NLECTC–Northeast is talking to the U.S. Air Force about adapting some of its C4ISR and data mining programs. As with other technology applications, it is a matter of piecing down the requirements to buy and set up the technology in compliance with U.S. and Canadian laws relating to data handling and information sharing.

Surveillance has always been a major element of border security, and it will continue to play a big role in IBET operations. Future IBET surveillance may take another lesson from the military and use unmanned aerial vehicles (UAVs). "In the meantime," Dilmore says, "RCMP has some pretty good air assets that are capable of doing limited types of surveillance. Nothing exotic, but it can input into a GIS receiver. Customs is looking at putting some air assets up there also [in the New York and Washington State areas]. Also, the Border Patrol has begun flying helicopters and fixed-wing aircraft."

Dilmore notes that because much of the northern border is under water, an effective border patrol must have a marine element. Joint teams working on waterways are called IMETs—Integrated Marine Enforcement Teams. The first IMET, at Blaine, combined air support from RCMP with water vehicles from the U.S. Coast Guard and U.S. Customs Service.

At Cornwall/Massena, the Border Patrol and RCMP have been running joint marine patrols as part of IBET. Although this has been effective, some smugglers craft still get through. The agencies have contacted NLECTC to help find techniques to intervene on marine pursuits. Different approaches are being evaluated, including a snare to entangle a boat. BTCT has tapped into federal expertise on vessel-stopping techniques, some of which are classified, and is working with the Coast Guard to secure release of some of these techniques for IBET use.

The IBET Scenario

Asked how September 11 changed things, Laun says, "The problems are the same; the stakes have been raised. The magnitude of the events have led us all to pursue enhanced security with greater vigor."

In addition to their normal border security operations, IBETs have been working on a three-level response plan they call the IBET scenario. Level one is normal day-to-day operations that focus on cooperative responses to routine border incidents and interdiction. The second level is joint surveillance operations based on intelligence gathering and developing such means of surveillance as UAVs. The third level is disaster preparedness.

Laun adds that more resources are available to IBETs than ever before. "Getting myriad organizations to blend and work together is easier now; September 11 has sharpened the focus on the need to become better and stronger partners than we've ever been," he says.

From the Canadian Side

"The IBET is always on," says Inspector Michael McDonell of the RCMP Cornwall Detachment. "We don't go on patrol without talking to the U.S. Border Patrol, the RCMP, the Mohawk Police, and the OPP [Ontario Provincial Police]. Border integrity is always an integrated effort. We always mirror the Border Patrol so they're never out there alone, nor are we. If the Border Patrol is chasing them over the border, we're here waiting for them."

RCMP wants to maximize the benefits of technology. "We want to be the first to take it from concept to practice," mostly by collating and analyzing broad technology and intelligence. NLECTC assistance with GIS and other command-and-control hardware and software is bringing IBET ever closer to this goal. But as McDonell says, "Every day we go to work, we realize how much more we need to do to cover the border."

But technology alone is not enough, McDonell says. The IBET approach is successful because it understands that human communication and teamwork remain the critical elements of success. "The key is breaking down the walls. We are looking at ways of colocating our people as well as exploiting technology."

For more information about Integrated Border Enforcement Team initiatives, contact Gordon Dilmore at the Border Research and Technology Center, 888-656-2782, or e-mail gdilmo@brtc.nlectc.org; or call Chris McAleavey, National Law Enforcement and Corrections Technology Center–Northeast, 888–338–0584, or e-mail chris.mcaleavey%3Com.com. Information is available at Integrated Border Enforcement Team newsletter, U.S. Attorney's Office, Northern District of New York, 315-448-0672, or peter.laun@wsgd.gov.
Before implementing electronic supervision, an agency should know that the potential of such technologies is best realized when used to supplement existing programs and that the chosen system must be in harmony with the agency’s values, vision, and mission to achieve optimal success. A needs and resource assessment process should look at the entire system to determine how electronic supervision would be most beneficial. Electronic supervision strategies may be appropriate at several points within the criminal and juvenile justice systems and for different classes of offenders. The assessment should also review the available technologies to see which form of electronic supervision might be most beneficial.

Additionally, the legal status of those who may be supervised with electronic technologies must be distinguished to plan appropriate program goals, strategies, and responses to violations. Prior to trial and adjudication, defendants are considered legally innocent, and their rights are protected from the power of the State even though they may be confined to ensure they appear for trial or to protect the public. Supervision with electronic technology may be substituted for pretrial confinement to achieve these same purposes. After adjudication, electronic supervision may be a useful tool to achieve goals of offender punishment and rehabilitation and public safety.

Further, policies and procedures that protect offenders’ due process rights must be in place before persons can be deprived of their freedom. As with other types of technology used in criminal justice cases, the technology must be accurate and meet scientific standards acceptable to courts. Should a revocation be based solely on the technological evidence, the methodology used must have a high degree of accuracy. Because of these issues, it is important that all parties set clear goals for each program.

A number of technologies currently available serve a variety of purposes in offender supervision. These include the following:

- **Automated Reporting Systems** may be most effective with low-risk, low-need offenders to simplify and streamline the supervision process while still holding the offender accountable. Automated reporting can take place through the use of a telephone or a computerized reporting system and is useful in that the offender’s identity and location can be recorded at the time of the report. These and other less restrictive supervision techniques can be used to reward offenders who have maintained consistent compliance throughout their period of supervision.

- **Identity Verification Devices** can range from personal identification numbers to biometric verification that recognizes different parts of the human body to ensure the reporting person is the intended offender.

- **Remote Alcohol Detection Devices** operate like a Breathalyzer®. The device—usually in the offender’s home—requires the user to blow into the device to measure blood alcohol content. When prompted, users must blow into the device for a long enough period of time to ensure that deep lung air is expelled. The results are recorded by a computer to determine compliance with no-alcohol conditions.

- **Ignition Interlock Devices** are linked to the electrical system of an automobile. This device also operates like a Breathalyzer®. The driver must expel deep lung air into the device in order to operate the vehicle. If the driver’s blood alcohol content registers above a predetermined level deemed unsafe to operate the vehicle, the vehicle will not start. This type of electronic supervision allows offenders to participate in society while reducing their risk of driving while intoxicated.

- **Programmed Contact Systems** are some of the most widely used types of electronic supervision tools; however, they do not all work alike. Although a wide variety of technologies is involved, programmed contact systems are all used to contact and verify the location of offenders in their homes or other locations. They may be used with offenders who are placed on home monitoring and must stay at home virtually all times, or they may be used for offenders who are restricted to their homes at various times but can come and go for approved activities. Programmed contact systems are automated calling systems. The backbone of these systems is a central computer that either receives telephone calls from or makes calls to the offender in one or more locations.

- **Continuous Signaling Devices** require the offender to wear a battery-powered transmitting device that emits a radio frequency signal two or more times a minute. The devices are placed on the offender’s wrist or ankle with a tamper-resistant strap and must be worn at all times. Manufacturers should incorporate tamper-resistant and alert features in their transmitters. A receiver is installed in the offender’s home attached to the telephone. The receiver detects the transmitter’s signals and conveys a message via a telephone report to a central computer either when it stops receiving the radio frequency or when the signal resumes.

(See Electronic Supervision, page 12)
TechoShorts is a sampling of article abstracts published weekly as part of the National Law Enforcement and Corrections Technology Center's (NLECTC's) online information service: the Law Enforcement and Corrections Technology News Summary.

Offered through JUSTNET, the website of NLECTC, this weekly news summary provides synopses of recent articles relating to technology developments and initiatives in law enforcement, corrections, and the forensic sciences that have appeared in newspapers, news magazines, and trade and professional journals. The summaries also are available through an electronic e-mail list, JUSTNETNews. Each week, subscribers to JUSTNETNews receive the summary directly via e-mail.

To subscribe to the JUSTNETNews/Law Enforcement and Corrections Technology News Summary, e-mail your request to asknlectc@nlectc.org or call 800–248–2742.

Note: Providing synopses of articles or mentioning specific manufacturers or products does not constitute the endorsement of the U.S. Department of Justice or NLECTC. Reproduction of this text is encouraged; however, copies may not be sold. The NLECTC Law Enforcement and Corrections Technology News Summary should be cited as the source of the information. Copyright 2002, Information Inc., Bethesda, Maryland.

Potato Technology May Help Move the Mail

Newspix (Federal Laboratory Consortium for Technology Transfer)

An effective tool against anthrax contamination may come from the same technology that brings whole-some Idaho potatoes to the family table. The U.S. Department of Energy's Idaho National Engineering and Environmental Laboratory (INEL) is teaming with a small business to explore the use of ozone to destroy anthrax. An Idaho-based company had developed a patented process to deliver high concentrations of ozone to freshly harvested potatoes as they travel along conveyor belts. The ozone destroys harmful bacteria and enables farmers to store their crops safely for months. INEL researchers believe this process also can sterilize mail and are testing their theory with harmless surrogates for anthrax spores.

Bees Learning Smell of Bombs With Backing From Pentagon

New York Times

Scientists backed by the Pentagon have experimented for 3 years with the use of bees to detect explosive residues, training them to ignore the scent of flowers and to focus on other smells instead. Using sugar as a reward, scientists have been able to train a whole hive of bees in less than 2 hours, noting that upon learning, bees somehow transfer their newfound knowledge to other bees quickly and efficiently. Initially intended for use in mine fields, trained bees could also be employed to find truck bombs and other hidden explosives. Recent testing found that bees were able to find explosive chemicals with a 99-percent accuracy rate. In such locations as a truck stop, a clustering of bees could alert officials of a possible explosive device, whereas in larger areas, tiny radio transmitters could be attached to individual bees, allowing officials to track them to a bomb's source. Though bees are highly effective as bomb detectors because of their extreme sensitivity to molecules and their ability to cover large areas and hard-to-reach places, they cannot be used at night or in rainy or cold weather.

Vocal Cameras Focus on Graffiti

Riverside Press-Enterprise

The Grand Terrace City Council in California has considered purchasing "talking" cameras to ward off graffiti vandals. The $3,500 cameras are bulletproof and can be customized to issue a loud 15-second warning message whenever they detect a person writing graffiti. The surveillance devices have been shown to drive gangs and vandals away from inner-city hangouts and parks, according to regional law enforcement officials. Grand Terrace assistant city manager Steve Berry says the camera could save the city thousands of dollars by reducing the cost of graffiti. He adds that city maintenance crews are forced to remove graffiti a couple of times a week, with each incident costing the city between $25 and $100 in materials and time. The cameras would be paid for out of funds received from the California Law Enforcement Equipment Program.

Program Helps Lost, Confused Get Back Home

Molesto Bee

"Homeward Bound," a new program unveiled by law enforcement officials and senior care advocates in Stanislaus County, California, will make finding missing elderly people and dependent adults easier. The program will establish a computer database of photos and other IDs of elderly people and adult dependents to which county law enforcement agencies will have access. Those who sign up for the free program must be at least 18 and have a mental or physical disability or an inclination to get lost or confused. The database will store identifying information, addresses, and names for at least 3 years and allow law enforcement officials access from computers in patrol cars and police stations. Stanislaus County law enforcement officials say police pick up lost elderly or disabled persons at least once a week, and the program will be a great help in quickly identifying their homes.

The Stanislaus Elder Abuse Prevention Alliance says the program will bring relief to families caring for elderly people and dependent adults.

Sandia Develops New Stun Grenade

Associated Press

A new stun grenade has been developed by New Mexico's Sandia National Laboratories (SNL) that the lab claims will be a safer way to stun kidnappers and terrorists so hostages can be freed. According to Mark Grubelich of SNL, the new stun grenade is less dangerous because the explosive fans out as a powder before igniting, creating a blinding and deafening, yet harmless, explosion inside a room. Furthermore, the canister does not suffer any damage and can be reloaded, making it useful in training and less expensive.

Computer Spy Methods Discovered in LED Lights

Reuters

Lockheed Martin Space Systems computer programmer Joe Loughry writes in an essay that he has discovered a low-tech way to snoop on computer data by studying the flashes of LED lights, which are featured on modems, key-boards, routers, and other kinds of electronic equipment. "It requires little apparatus, can be done at a considerable distance, and is completely undetectable," he explains. All that is necessary is a telescope viewer and a way to process the signal. Loughry says that he could read an optical signal from about 22 yards away with an optical sensor, and notes that LED-enabled devices most susceptible to this form of eavesdropping are those used in low-speed, long-distance networks, such as those found in electronic banking machines. It is relatively simple to prevent such spying by keeping equipment out of sight, obscuring LEDs, or shutting them off when inactive.

Training Cues for the People in Blue

KM World Online

Since December 2001, officers in North Carolina's Charlotte-Mecklenburg Police Department have used a learning management system (LMS) to enroll more than 1,500 of the department's 1,500 officers have used the system, which provides officers a calendar of mandatory courses offered online. Since its inception, about 1,000 of the department's 1,500 officers have used the system, which provides officers a calendar of mandated courses. Officers can enroll in other classes, including offline courses, via the LMS, and view procedural changes from their own home page. In the future, the department plans to put some of its courses online, covering topics ranging from hazardous materials to diversity training to radar certification, as well as tools that will help officers with their career plans. The system, which securely records officers' training histories, will also help supervisors choose qualified personnel for specific roles.

Lethal Fence Proposed for Maximum Security Prison

Associated Press

Arizona's Department of Corrections has asked the State legislature for permission to build a $600,000 high-voltage fence at its prison facility in Florence, Arizona. According to department officials, at least seven other States currently use high-voltage fences at their prisons, but no State prison in Arizona has been equipped with such a fence. The installation would allow the Depart- ment of Corrections to save $734,000 a year, according to Chuck Ryan, deputy director for prison operations.

Wells Fargo Brings in New Scanners To Catch Fake Money

Minneapolis Star Tribune

A new ultraviolet scanner is helping Wells Fargo® analyze drivers' licenses, checks, cash, and other documents to verify their authenticity. Due to security concerns, the bank chose not to reveal how the scanners work, but the ultraviolet equipment "already has paid significant loss-prevention dividends," according to Jon Campbell, regional president of Wells Fargo's Minnesota branch. A survey by the American Bankers Association finds that phony cash and checks are becoming one of the most widespread frauds in the United States. Law enforcement officials estimate $12 billion to $18 billion in annual losses due to counterfeit money. In addition to the ultraviolet scanners, the bank uses thumbprint readers, software that detects problematic accounts, and training programs that identify con games.
Online News Summary includes article abstracts on law enforcement, corrections, and forensics technologies that have appeared in major newspapers, magazines, and periodicals and on national and international wire services and websites.

Publications from NIJ and NLECTC that you can view or download to your system.

Frequently Asked Questions that offer detailed information based on thousands of calls to our information specialists.

Calendar of Events that lists upcoming meetings, seminars, and training.

Links that can take you to other important law enforcement and corrections websites.

For help in establishing an Internet connection, linking to JUSTNET, or finding needed technology and product information, call the NLECTC Information Hotline at 800–248–2742.

Don’t get caught without TechBeat!

Individual Subscriptions: TechBeat is available at no cost. If you are not currently on our mailing list or need to change your mailing label information, please call us at 800–248–2742 or e-mail us at asknlectc@nlectc.org.

Domestic Department Subscriptions: If your division, department, or agency has more than 25 individuals, we can drop ship as many copies as you require. All you have to do is provide us with the quantity needed, a shipping address (no post office boxes, please), and a contact name and telephone number. Your only obligation is to disseminate them once they arrive. If you require fewer than 25 copies, please provide us with the names and addresses of individuals who are to receive the newsmagazine and we will send copies directly to them. Contact Rick Neimiller, TechBeat managing editor, at 800–248–2742, for additional information or to subscribe.

Article Reproduction: Unless otherwise indicated, all articles appearing in TechBeat may be reproduced. We do, however, request that you include a statement of attribution, such as: “This article was reproduced from the fall 2002 issue of TechBeat, published by the National Law Enforcement and Corrections Technology Center, a program of the National Institute of Justice, 800–248–2742.”

Questions/Comments/Story Ideas: We welcome all questions, comments, and story ideas. Please contact Rick Neimiller, TechBeat managing editor, at 800–248–2742 or e-mail rneimiller@nlectc.org.

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

Photo Credits: Photos used in this issue of TechBeat copyright © Arvöville; Photodisc, Inc.; Corbis Stock Market; Eyewire; The Ottawa Sun, photographer Errol McGihon; the Los Angeles County Sheriff’s Department; and Aspen Systems Corporation.

The National Law Enforcement and Corrections Technology Center is supported by Cooperative Agreement #96–MU–MU–K011 awarded by the U.S. Department of Justice, National Institute of Justice. Analyses of test results do not represent product approval or endorsement by the National Institute of Justice, U.S. Department of Justice; the National Institute of Standards and Technology, U.S. Department of Commerce; or Aspen Systems Corporation. Points of view or opinions contained within this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, Bureau of Justice Statistics, Office of Juvenile Justice and Delinquency Prevention, and Office for Victims of Crime.

TechBeat is the award-winning newsmagazine of the National Law Enforcement and Corrections Technology Center (NLECTC) system. Our goal is to keep you up to date with technologies currently being developed by the NLECTC system, as well as other research and development efforts within the Federal Government and private industry. TechBeat is published four times a year.

Managing Editor, Rick Neimiller; Contributing Editor/Writer, Lois Pilant; Contributing Writers, Anne Crowe, Becky Lewis, and Karen Sherman; Editor, Michele Coppola; Assistant Editor, Brian Higgins; Graphic Designers, C. Denise Collins and Tina Kramer.
T

irty-plus years ago, when police radios were underpowered and cumbersome, one officer voiced his irritation about his inability to communicate with fellow officers this way: “Mission Control could talk to astronauts on the moon, but we couldn’t talk to our partners around the corner, less than a block away.”

Today police radios are certainly smaller and much more powerful. But improvements in technology have not eliminated the issue of interoperability—the capability of public safety agencies at all levels to communicate across jurisdictions. This lack of interoperability among agencies, emergency medical services, and fire departments operating on different frequencies, use different equipment, and follow different policies and procedures, making communication and coordination between agencies and across jurisdictions very difficult.

Interoperability is a complex situation that has been evolving over the years,” says Tom Coty, AGILE program manager. “It’s complex not only because of the sheer number of agencies, but also because they are in different points in the life cycle of their equipment. One may have a brand new system, while another nearby agency has equipment that is 15 to 20 years old.”

According to Coty, most public safety professionals would say they have experienced problems communicating with others in their field. Each agency, however, faces different interoperability issues, such as outdated equipment and no funds to buy new equipment, city police and fire department radios that operate on different frequencies, cell phones that allow different agencies to talk to one another, but have significant access problems during critical events; and existing communication links between agencies, but no policies or procedures that cover when and how to use them.

For most public safety agencies, Coty says, the biggest problem stems from incompatible radio frequencies and lack of funds to buy new equipment.

The Federal Communications Commission (FCC) licenses radio frequencies for all non-Federal users of radio spectrum, including public safety agencies, commercial radio and television stations, business radios and more. The spectrum is a range of frequencies used for communications. It is divided into channels, 10 of which are for public safety agencies’ use.

Within those bands, the FCC licenses the frequencies or channels used by each agency. Frequency is measured in terms of millions of cycles per second, or megahertz (MHz).

No commercially available radio equipment in all 10 hands would be able to communicate with each other. Some radios made by different manufacturers cannot even communicate within a department with its own radio band. This leads to temporary “islands,” thus, installing numerous radio antennas in ambulances and patrol cars so their occupants can talk to everyone else in an area. Another commonly used fix, the dispatch relay, uses a third party to relay messages from one agency to another. These solutions are cumbersome and expensive. They use up precious time that could allow a suspect to escape or a fire to spread.

Technology solutions to interoperability problems are becoming more common. One solution employs a crossband repeater system, which receives a transmission on one frequency and automatically retransmits it on a different one. Unfortunately, law enforcement and other public safety agencies often do not know which new technologies can help them, or even that these technologies exist.

In 1994, NIJ’s National Law Enforcement and Correction Technology Center (SELECT-J) Rocky Mountain completed an intensive study of interoperability issues. States and Local Law Enforcement Wireless Communications and Interoperability: A Quantitative Analysis. NIJ used the study to launch the AGILE program, which coordinates all NIJ interoperability initiatives into a coordinated effort to help Federal, State, and local law enforcement agencies communicate and share information. AGILE originally stood for Advanced Generation of Interoperability for Law Enforcement, but its target audience has expanded to include all public safety agencies.

“AGILE facilitates information sharing and provides support to professionals, giving them the ability to help themselves,” Coty says. Nationally, that can mean more than 30 million transactions and interactions, and their leaders, locally, it can mean offering one-on-one technology assistance or developing a three-part approach to implement its mission:

- Research, development, testing, and evaluation technology solutions.
- Standards identification, development, and adoption.
- Outreach and technology assistance.

No single fix can solve complex interoperability issues for everyone. Coty says. At any point in time, AGILE staff have more than 30 projects and initiatives under various stages of development. One of them may provide just the solution an agency needs.

Coty says public safety personnel often learn about new technologies by seeing a demonstration at a conference or by hearing about new equipment in a market. Agencies may not know who developed the technology, whether it will work with their systems, or where to find out more about it. They can begin their research on the AGILE website at www.agileprogram.org.

The AGILE site includes a section that lists site updates and the latest interoperability news. The site provides access to AGILE reports and printed materials and offers online guidance on finding, understanding standards, the National Task Force on Interoperability, and a list of related links. It also provides updates on AGILE research projects, including the following:

- ACU-1030 Soft furnishings. The City of Alexandria (Virginia) Police Department has served as a test bed for several potential interoperability communications solutions, including the ACU-1030, an audio gateway that lets the co-workers incorporate radio systems. The ACU-1030 provided coverage for the inauguration of President George W. Bush. Linking to the U.S. Secret Service, the U.S. Capitol Police, the Federal Bureau of Investigation, and other agencies, Alexandria will soon test two new systems. A Motorola product to link Motorola technology, and Incident Command Radio Interface (ICI), a Communications Applied Technology product. Although similar to the ACU-1030, the portable ICI system can run in broadcast-stand alone or AA batteries to up 24 hours.
- CAPAD. In the Balanced Budget Act of 1997, Congress directed the FCC to reallocate 24 MHz of spectrum in the 700 MHz band for public safety use. Now used by CPB television channels 60 to 69, this spectrum will be available within the next several years. Utilization of the release of this spectrum, the National Public Safety Telecommunications Council (NPSTC) and the Public Safety Communications Research Council requested the development of a Computer-based Presentation Resource and Database (CAPRAD) to facilitate interoperable coordination in the all-important frequencies. NPSTC-Rocky Mountain recently completed this database, which will have secure Internet access, and is now working on database distribution and orientation.
- CAPRIN. Several years ago, a man committed suicide by jumping from the Capital’s Woodrow Wilson Bridge. Agencies in Maryland, Virginia, and the District of Columbia ran into numerous interoperable problems while trying to coordinate rescue efforts and arrange a real-time radio support team. The incident, among others, triggered the request to create the Capital Wireless Interconnected Network (CAPWIN). CAPWIN will integrate existing voice and data communication systems into the Nation’s first multi-integrated wireless voice network designed to facilitate transportation, and public safety. Research and development are now underway at the Universities of Maryland, the University of Virginia, and George Mason University. The goal is to establish this network a model that can be replicated in other regions of the country.
- COPUPN. Developed through a joint effort between the University of Arizona and the Tucson Police Department, COPUPN Knowledge Management System software uses the Internet to link member databases. The COPUPN Connect module allows multi-media training sharing across a network of record management systems that use different software and parameters. The COPUPN Detect module provides advanced data analysis. For example, one can search for information on wireless loss and calls information on sex offenders located to frequent school playgrounds, then search for witnesses for the FBI.
- IMPACT. IMPACT is an NIJ research and development project completed in FY 2001. Developed tools and technologies to integrate disparate legacy systems to permit information sharing with appropriate security/privacy. Software and data models from this project are newly available.
- INFOTECH. INFOTECH has an NIJ research and development project completed in FY 2001, developed tools and technologies to integrate disparate legacy systems to permit information sharing with appropriate security/privacy. INFOTECH software and technology are now available at www.agileprogram.org.

Interoperability Technology

Just as the research and development portion of AGILE includes many components, its Standards Project analyzes and reviews standards related to all of the above and telecommunication assistance. The project’s goal is to identify and create a comprehensive interoperability standards for NIJ adoption. Coty says that although some new standards may need to be developed, most interoperability standards already have been created by such organizations as the Telecommunications Industry Association (TIA) through the development of the National Association of Public Safety Communications Officers (NAPCO); the National Security Telecommunications and Information Systems Board (NSTIC) and the National Telecommunications and Information Administration (NTIA) are working to develop a model that can be replicated in other regions of the country. INFOTECH staff are helping to develop software. INFOTECH software and technology are now available at www.agileprogram.org.

Interoperability Standards

AGILE outreach, like research and development and standards development, encompasses many elements. Outreach includes the website, conference presentations, and telephone assistance. Additionally, in response to requests from public safety agencies, AGILE distributes reports to assess agencies’ capabilities and propose solutions. Coty says, “Often, a lot of the solutions are really simple. For example, the agency may be dealing with vendors who sell equipment. We send out an engineer who will sit at the radio transmissions and show them what is wrong. This report has only been implemented in one region.”

Technical experts also visit sites once the equipment is in place. Coty says. After the equipment is set up, it is important that the agency work out agreements with other nearby departments to provide support in a new deployment, and practice and train for its use. Outreach and assistance projects include:

- National Task Force on Interoperability. In an effort to improve public safety radio communications, a National Task Force on Interoperability was created. The task force’s efforts are guided by Federal and state leadership and representatives from the public safety community. Its goal was to review public safety wireless interoperability in the national law and give us the opportunity to develop a list of actions that could be taken to overcome the policy barriers to improving public safety interoperability.

The forum received such a positive response that NIJ continued the effort by funding a TIA/European Telecommunications Standards Institute (ETSI) model that can be replicated in other regions of the country.

- NPSTC Support Office. AGILE also funded the creation of the NPSTC Support Office (NSO) in FY 2000. NSO’s role is to provide technical support and funding for new equipment. The NSO will develop a technology model that can be replicated in other regions of the country.

- NPSTC Support Office. AGILE also funded the creation of the NPSTC Support Office (NSO) in FY 2000. NSO’s role is to provide technical support and funding for new equipment. The NSO will develop a technology model that can be replicated in other regions of the country.

- Interoperability Assessment for the State of Texas. In conjunction with the Sheriffs’ Association of Texas and the State of Texas, AGILE is surveying the existing state structures and preparing proposals to interoperability issues. In addition to building partnerships at the state and local level, this project will develop a how-to guide for implementing interoperability projects.

- Technology standards, outreach and assistance and up to $600,000 to AGILE’s mission to solve the problems related to interoperability, problems that also include a lack of available spectrum and funding for new equipment. "Technology isn’t the stumbling block," Coty says. "You can overcome technology issues. The real hard task is working out the policies and their day-to-day execution.”

For more information on AGILE, visit the AGILE website at www.agileprogram.org.
on the surface it seems a quiet place. Ordinary looking offices are filled with desks, computers, and bookshelves. People go about their business at a focused, measured pace. Windows look out on trees, ponds, and grassy fields. Deer and geese make their home here. It is about as far removed from city streets and cellblocks as you can get.

But within this quiet, unassuming place, research and analysis take place to increase the safety and efficiency of police, corrections, and public safety personnel throughout the United States. Located in the Maryland suburbs, 25 miles from downtown Washington, D.C., is a complex of buildings and laboratories situated on a 578-acre campus. This is the headquarters of the National Institute of Standards and Technology (NIST) and home to the Office of Law Enforcement Standards (OLES), which is funded by the National Institute of Justice (NIJ).

Every day at OLES, work proceeds on a number of technology-related projects and programs, including the following, to benefit the public safety community.

MATCHING BULLETS

When people need a quick, all-encompassing solution, they speak of searching for a magic bullet. At OLES, they do not yet have a magic bullet, but they do have one.

Just as no two fingerprints are alike, each firearm has its own set of unique characteristics that leaves a signature on the bullets and casings it fires. Forensic examiners analyze these ballistic signatures to connect a firearm to bullets or casings found at crime scenes. Susan Ballou, program manager for forensic sciences at OLES, explains that most ballistics laboratories use the Integrated Ballistics Identification System (IBIS) to match bullets. IBIS uses image capture, image analysis, and nationwide databases to match bullets to firearms. High-quality measurement standards for bullets and casings are necessary to maintain the system’s reliability. To help laboratories maintain these high standards, NIST developed the Research Material 8240 Standard Reference Material (SRM) bullet. An SRM has had specific values verified and is certified by NIST.

“The bottom line is to see it from a forensics point of view,” Ballou says. “I usually bring in DNA as an example, since it is such a hot topic. When we started forensically using DNA around 1987, every lab began incorporating it to the best of its ability. When different pieces of evidence from the O.J. Simpson case were sent to different labs, it brought to light that we had this highly sensitive type of evidence and we needed to make sure that everybody was following the same procedures. If you tested something in one lab, you needed to be able to substantiate how you got the same result in another. They decided they needed to put standard operating procedures in place.”

Matching bullet signatures has the potential for the same types of problems, Ballou says. Forensic labs are encouraged to submit images of bullets they test to IBIS’s national database. This database enables a lab to match the signature of a bullet recovered from a crime scene in Mississippi with that of a match found at a crime scene in Kansas. If Kansas law enforcement officials have the gun, it might help solve the Mississippi crime. However, slight differences in the calibration of equipment make matching bullet signatures harder. “It seemed that nobody was doing the exact same thing to their bullet images, so the success rate of the database search wasn’t as high as it should have been,” Ballou says.

Recognizing the need for nationwide calibration, then-Attorney General Janet Reno backed a 1998 initiative for NIST that provided startup funds to create the SRM bullet. “If you buy a box of ammunition off the shelf, there can be so many differences,” Ballou says. “They’re microscopic and won’t be visible to the naked eye, but they may make a big difference in testing.”

A standard, computer-generated bullet will soon be available from NIST at a cost of approximately $2,000. (The price may be reduced depending on the result. NIST, which does not make a profit from the sales, recycles the funds into creating additional bullets.) This standard bullet is reproduced through a numerically controlled diamond-turning technique from master bullet signatures stored in a computer. A forensic laboratory can use this reproduction to calibrate its equipment settings. This will reinforce consistency both within IBIS and among laboratories, leading to greater success in finding matches.

At first, Ballou says, the IBIS developer did not see the need for an SRM. A company representative told her that if a lab examiner followed directions for setting up the equipment, it would be properly calibrated. However, Ballou says, those directions do not allow for such variables as differences in light selection and an examiner’s individual preferences, which might lower a lab’s match success rate. The database might offer too many bullet images as possible matches, requiring the examiner to spend time doing visual searches. A lab might have time to follow up on only five, and the sixth might be the match, she says.

NIST’s first run produced 40 SRM bullet reproductions. Of these, 20 will be available to forensic laboratories and 20 will remain at NIST for teaching purposes. OLES plans a workshop and a series of presentations on how to use the standard bullet. Because production is labor intensive and costly, NIST will not keep a large inventory of the bullets, but it will produce more if labs request them. The Bureau of Alcohol, Tobacco and Firearms and the Federal Bureau of Investigation (FBI) have taken part in the testing and other phases of this project. A final report is being prepared.

STANDARDIZING BOMB SUITS

In contrast to the standard bullet project, which is wrapping up, the bomb suit standards project is just starting, according to Kirk Rice, program manager for weapons and protective systems at OLES. The objective of this study is to establish minimum performance requirements and testing methods for bomb suits that are used by explosive ordnance disposal (EOD) personnel. Rice recalls his initial surprise that the military did not have such a standard, although the U.S. Army has preliminary performance requirements that can be used as a starting point.

Rice says purchasing agents typically rely on advice from others in the field and on manufacturers’ literature; therefore, the EOD community has identified development of a standard as a top priority. The project will involve consulting with explosives experts to identify essential features of bomb suits, devising rating categories, proposing a standard, validating it through testing, and submitting the standard for comment and review.

The Technical Support Working Group (TSWG), an interagency government organization, helps provide overall coordination and access to resources from other countries. At this point, Rice says, the parties involved are considering the scope of the study and which suits to analyze, defining typical threat levels, and ensuring consistent testing standards. OLES also will seek input from the medical community about the human body’s ability to withstand blast pressure.

“All these State and local police are dealing with pipe bombs, with things that show up at city hall and at abortion clinics. They don’t have the resources to go out and test suits and make an educated decision,” Rice says. “Sometimes they’re not even sure what a bomb suit is. The FBI says they get calls from local police who ask if they put on body armor and a protective helmet, is that a bomb suit, and if so, can they wear that to come take disarmament training? That’s why NIJ is taking it under its wing.”

A bomb suit is designed to deflect much of the force from a blast around the body instead of the body’s taking it all at one point. If someone is wearing the wrong equipment or wearing it incorrectly, he says, the blast force could hit the officer under the chin and break his or her neck.

“In generic terms, a bomb suit is a protective suit designed to shield the wearer from blast and fragment damage from explosive devices,” Rice says. The goal of the project is to determine the extent to which a specific suit shields its wearer.
and rate it on a standard threat scale. Although this sounds similar to existing NIJ body armor standards, Rice thinks the need is not as widespread.

Rice and the rest of the group working on the project will have a lot of data to go through, but they can draw comfort from the knowledge that most manufacturers already produce good bomb suits. “It isn’t that officers are wearing bomb suits and they’re not working; they are,” Rice says. “The idea is just to make it easier for law enforcement agencies to pick what’s right for them. Manufacturers welcome this research. Right now, they make a product, and they make what they think is needed. A standard will give them a benchmark to shoot for.”

Rice says OLES has met with a group that included representatives from the National Bomb Squad Commanders’ Advisory Board, the FBI Bomb Data Center, the U.S. Army, TSWG, and the Navy EOD school to discuss the scope of the project. TSWG plans to convene a working group of professionals later in 2002. The project is expected to take approximately 2 years to complete.

**TESTING SALIVA**

The bomb suit standard will better protect law enforcement personnel. But Dr. Alim Fatah, OLES program manager for chemical systems and materials, is leading a study that may lead to more accurate drug testing results while protecting arrestees’ and inmates’ civil rights.

In recent years, many have felt that watching a subject produce a urine specimen for drug testing invades his or her privacy. But if someone is left alone to produce the sample, samples can be swapped or otherwise contaminated. Saliva, however, can be collected under full observation without invading a subject’s privacy. Research has shown that saliva appears to reflect blood-drug concentrations accurately. According to Fatah, studies have shown that many therapeutic drugs and drugs of abuse (e.g., amphetamines, marijuana, cocaine, opiates, LSD, and PCP) can be detected in saliva.

Under OLES’s direction, researchers at the University of Utah’s Center for Human Toxicology compared the presence of codeine in blood to that in saliva. Fatah says results showed that saliva concentrations were higher, easier to detect, and present longer. Saliva used in this study was acquired through spitting.

In a related study, the researchers looked at devices that collect saliva samples from inside the cheek. They also looked at the results when saliva production is stimulated by sucking on a lemon drop or chewing paraffin wax. Spitting produced uniformly higher results, Fatah says. He notes that one drawback to using saliva is the potential for contamination when the person being tested took a drug by mouth, inhalation, or smoke and then ate, drank, or smoked other substances.

**ANALYZING PEPPER SPRAY**

Fatah also is studying human reaction to pepper sprays. Oleoresin capsicum (OC), the oil extracted from the cayenne pepper plant, is the active ingredient used in most self-defense sprays. Although pepper sprays are a useful and purported nonlethal form of defense, commercially available products vary widely in their strength and potential effectiveness.

Law enforcement, corrections, and the public have concerns about product performance, legal issues, and medical safety surrounding the use of pepper sprays. OLES has undertaken a study to produce data for use in developing minimum pepper spray performance standards. Manufactures’ standards and product performance vary widely, sometimes even from batch to batch of the same product produced by the same manufacturer, Fatah says. Some pepper spray products have been shown to vary by 10 to 20 times in the amount of OC used.

The first phase of the study, conducted by researchers at the University of Utah’s Center for Human Toxicology under the direction of OLES, analyzed several products made by different manufacturers. Some sprays contain only synthetic capsaicin (nonivamide), others contain natural substances from a variety of peppers, and others mix synthetic and natural capsaicins. (Capsaicin is the active ingredient in capsicum.) An analysis of 10 sprays showed wide variations in the amounts of OC used. The spray with the strongest concentration had about 40 times the amount contained in the weakest spray. Several samples appeared to be the same product but had different lot numbers. Fatah says that the next step is to determine the effectiveness of these various concentrations and to recommend standards.

To learn more about standard bullets, contact Susan Ballou at 301–975–8750, susan.ballou@nist.gov; about bomb suit standards, contact Kirk Rice at 301–975–8071, kirk.rice@nist.gov; and about saliva and pepper spray testing, contact Alim Fatah at 301–975–2753, alim.fatah@nist.gov. For information about the National Institute of Standards and Technology, log on to www.nist.gov; for the Office of Law Enforcement Standards, go to www.eeel.nist.gov/oles.
Technology can significantly enhance the effectiveness and efficiency of law enforcement, corrections, and forensic sciences. Just as important, it can help ensure public safety. But the incorporation of new technology can be complicated and require significant research, while inappropriate or underutilized technology can be costly—not only in money but also in time and public perception.

The National Law Enforcement and Corrections Technology Center (NLECTC) system, a program of the National Institute of Justice, can help agencies large and small when it comes to implementing current and emerging technologies. NLECTC serves as an “honest broker” resource for technology information and support at no cost.

Because most of this country’s law enforcement and corrections services are provided at the local level, the NLECTC system is composed of five regional centers and is complemented by several specialty offices and a national center. These centers and offices are co-located or supported by federally funded technology partners so they can leverage unique science and engineering expertise.

Contact NLECTC for:

Technology Identification
As an agency’s first stop in its search for new and developing technologies, NLECTC provides information relating to availability, performance, durability, reliability, safety, ease of use, customization capabilities, and interoperability. This information helps an agency determine the most appropriate and cost-effective technology to solve an operational problem.

Technology Assistance
Because most law enforcement and corrections agencies do not have access to technical experts and sophisticated equipment, NLECTC staff serve as proxy scientists and engineers. Areas of assistance include evidence analysis (e.g., audio, video, computer, trace, and explosives), systems engineering, and communications and information systems support (e.g., interoperability, propagation studies, and vulnerability assessments).

Technology Implementation
The implementation of technology can bring on a new set of concerns, from hardware/software compatibility to operational procedures and training. NLECTC helps develop procedures, protocols, and training materials. Generic guides, best practices, and information manuals often are leveraged from these hands-on assistance projects and made available to other agencies.

Technology/Property Acquisition
For most small departments, the acquisition of equipment to run day-to-day operations or outfit officers is a constant concern. NLECTC helps departments small and large take advantage of surplus property programs that make federal excess and surplus property available to law enforcement and corrections personnel at little or no cost.

Standards and Testing/Technology Evaluation
NLECTC oversees a standards-based testing program in which equipment such as ballistic and stab-resistant body armor, double-locking metallic handcuffs, and semiautomatic pistols is tested on a pass/fail basis. NLECTC also conducts comparative evaluations—testing equipment under field conditions—on patrol vehicles; patrol vehicle tires and replacement brake pads; and cut-, puncture-, and pathogen-resistant gloves. These evaluations allow agencies to select equipment that best suits their needs. On request, NLECTC evaluates new products to verify manufacturers’ claims.

Technology Demonstration
NLECTC introduces and demonstrates new and emerging technologies through such special events, conferences, and demonstrations as the Mock Prison Riot (technologies for corrections), Operation America (bomb-detection technologies), and an annual public safety technology conference. On a limited basis, NLECTC facilitates deployment of new technologies to agencies for operational testing and evaluation.

Capacity Building
NLECTC provides hands-on instruction in the latest technology solutions, primarily in the areas of crime and intelligence analysis, geographic information systems, explosives detection and neutralization, inmate disturbances and riots, and computer crime investigation.

Technology Commercialization
Bringing research and private industry together to put affordable, market-driven technologies into the hands of law enforcement and corrections personnel is another focus of NLECTC. Law enforcement and corrections professionals, product and commercialization managers, engineers, and technical and market research specialists identify new technologies and product concepts, then work with innovators and industry to develop, manufacture, and distribute these new, innovative products and technologies.

Technology Needs Assessment/ Prioritization
A national body of criminal justice professionals—the Law Enforcement and Corrections Technology Advisory Council (LECTAC)—influences the work of the NLECTC system by identifying research and development priorities. In addition, each regional facility has an advisory council of law enforcement, corrections, and forensics professionals. Together, LECTAC and the regional advisory councils help keep the NLECTC system attentive to real-world technological priorities and the needs of law enforcement and corrections. Created in 1994 as a program of the National Institute of Justice’s (NIJ) Office of Science and Technology, the NLECTC system’s goal, like that of NIJ, is to offer support, research findings, and technological expertise to help State and local law enforcement and corrections personnel do their jobs more safely and efficiently.
In addition to funding the National Law Enforcement and Corrections Technology Center–National, the National Institute of Justice (NIJ) supports the National Criminal Justice Reference Service (NCJRS), an international clearinghouse on crime and justice information. NCJRS staff respond to reference questions, provide referrals to other resources, distribute NIJ and other Office of Justice Programs (OJP) documents, and maintain a mailing list of more than 45,000 registered users. NCJRS sponsors a calendar of events at www.eventcalendar.ncjrs.org, which lists conferences and meetings of interest to the criminal justice community. If you are interested in signing up for the NCJRS mailing list, you may request a registration form using any of the following methods:

- **Fax-on-Demand.** Dial 800–851–3420, select option 1, then option 1 again. The registration form is #1 on the document index. The form will be faxed to you immediately.
- **Fax.** Fax your request for a registration form to 410–792–4358. You will receive a form promptly in the mail.
- **Online.** Go to www.ncjrs.org/puborder and request registration form BC640. It will be sent to you in the mail. Or register online at www.ncjrs.org/register.
- **Write.** Send a written request to NCJRS, P.O. Box 6000, Rockville, MD 20849–6000.
- **Call.** Call an NCJRS information specialist at 800–851–3420 and request a registration form.

As a registered user, you will receive the bimonthly NCJRS Catalog, the NCJRS Users Guide, and news and announcements of new publications and resources based on your criminal justice interests.

For more information about NIJ and NCJRS, visit their websites: www.ojp.usdoj.gov/nij and www.ncjrs.org.

---

**OFFICER SAFETY**

*Selection and Application Guide to Personal Body Armor, NIJ Guide 100–01.* This guide explains how to proceed when selecting and purchasing body armor. It responds to commonly expressed concerns and provides information to determine the level of protection required by law enforcement officers. It provides information on the latest ballistic-resistant standard (NIJ Standard–0101.04) and on the new stab-resistant standard (NIJ Standard–0115.00).

*Surviving a Shooting: Your Guide to Personal Body Armor.* This 19-minute videotape provides a synopsis of the National Institute of Justice's publication titled Selection and Application Guide to Police Body Armor. Covered in the videotape are what body armor is, what it can and cannot protect against, how to select it, and how to wear and care for it.

**VEHICLE TESTING**

*Michigan State Police Tests 2003 Patrol Vehicles.* This bulletin summarizes the test results from the Michigan State Police 2003 model year patrol vehicle evaluations.

*2003 Model Year Patrol Vehicle Testing.* This report contains the complete results of comprehensive tests conducted by the Michigan State Police of 2003 model year police patrol vehicles. Vehicles were subjected to major tests and evaluations, including vehicle dynamics testing, acceleration and top-speed testing, brake testing, ergonomics and communications evaluations, and fuel economy evaluations.

*Equipment Performance Report: 2001 Patrol Vehicle Tires.* This report presents the complete results of NIJ’s 2001 comprehensive evaluation of patrol vehicle tires. The report presents information to help law enforcement agencies decide which tires would be best for their patrol vehicle fleets.

To obtain any of the above publications, write NLECTC, P.O. Box 1160, Rockville, MD 20849–1160; telephone 800–248–2742.

Publications can also be downloaded from JUSTNET at www.justnet.org.
Receivers can detect transmitter signals from a range of up to, and in some cases exceeding, 150 feet when installed in a typical home environment. Receivers also should have tamper-resistant features to deter offenders from moving or disabling them.

**Victim Alert/Notification Systems** are most often used for domestic violence victims. This type of system enables victims to know when the offender is approaching their residence. A variation of the continuously signaling devices has been developed for victim alert and notification and offender compliance with stay-away orders. A transmitter is worn by both the offender and the victim and a receiver is placed at both residences. If the offender approaches the victim’s home, the system will provide notification of the offender’s presence.

**Field Monitoring Devices**, or “drive-by” units, are another type of continuous signaling technology. Probation or parole officers or other authorities use a portable device that can be hand held or used in a vehicle with a roof-mounted antenna. When within 200 to 800 feet of an offender’s ankle or wrist transmitter, the portable device can detect the radio signals of the offender’s transmitter.

**Group Monitoring Units** allow supervisors to monitor several offenders in the same location. This might be appropriate for tasks such as verifying attendance of multiple offenders in a day-reporting program or monitoring offenders confined in a residential group setting. Each offender in a group setting wears a transmitter to allow for electronic supervision by a stationary or portable receiver unit.

**Location Tracking Systems**, also known as global positioning systems, use 24 satellites orbiting the earth and are among the most complex electronic monitoring systems. The hardware for this system consists of a transmitter worn by the offender, a portable tracking device that the offender must carry or be near at all times, and a charging unit for the portable tracking device that stays in the offender’s home. Receivers detect signals from the satellites that include the exact time the signal is sent and the identity of the satellite sending the signal. This information is processed to determine the person’s location. This more expensive technology is usually employed with high-risk offenders. It can determine when an offender leaves an area where he should be (inclusion zone) or enters an area where he should not be (exclusion zone).

Although the use of electronic supervision tools is multifaceted and detail oriented, the measure of the effectiveness of the program will take place after implementation. As such, the human element in the implementation of an electronic supervision system should not be downplayed. The role of technology is to generate information; the decisionmaker is the one who must decide how that information should be used. Sound decisions must be made based on information gathered by these systems. Without sound policy and decisionmaking, information gathered from such systems is of minimal value.

“Electronic monitoring is just a supervision tool and in no way replaces the supervising officer,” says Eric Hanselman of Tracking Systems Corporation. “If an electronic monitoring program does not have clear goals, if the supervising officer’s caseload is too large to permit proper analysis of electronic monitoring data; or if sanctions for noncompliance are not defined, readily available, and implemented when necessary, the success of the electronic monitoring program may be lessened.”

The issues in this article were discussed by a 21-member working group of criminal justice professionals and are outlined in *Offender Supervision With Electronic Technology*, a report prepared by the American Probation and Parole Association (APPA) under a cooperative agreement funded by the National Institute of Justice. The report discusses assessment, planning, procurement, and technical steps needed to implement an effective electronic supervision program. To obtain a copy of the report, call APPA at 859-244-8207 or download it off the APPA website at [http://www.appa-net.org/embook.pdf](http://www.appa-net.org/embook.pdf).