Technology: Alaska to the Appalachians

The Rural Law Enforcement Technology Center (RULETC) in Hazard, Kentucky, will provide technology and technical solutions to a historically underserved population—the country’s rural, small town, and small county criminal justice agencies.

NLECTC–Northwest and RULETC are the two newest facilities to join the NLECTC system. In addition to their own focus areas, the two centers will work with the other centers to provide objective advice and technology assistance.

RULETC will enhance capacity building for isolated and rural agencies, provide crime mapping capabilities and long-distance learning opportunities, enhance the interoperability of communications systems, and share best practices and lessons learned.

Small agencies can only try what they think might work," Griffiths says, "and, if it doesn’t work, they’ve wasted their money. If it does work, they need to share that information. One of NLECTC–Northwest’s missions is to pass on the lessons departments have learned about equipment and strategies that work in extreme weather and geography.”

Transportation Challenges. Extreme cold, ice, and snow affect how police get around, Griffiths says. When it’s 50 degrees below zero, officers keep cruiser engines running. This results in wear and tear and makes the cruisers more vulnerable to theft. If the cruisers are turned off, the oil and transmission fluid become too viscous in the extreme cold.

In addition, most cruisers are equipped with studded tires for driving on ice. The Anchorage Police Department, he says, extensively tested studded tires and found that they were not particularly functional. Griffiths says his center would like to work with the Office of Law Enforcement Standards to test winter tires in adverse conditions.

According to Griffiths, 30 percent of Alaska’s population lives in communities that cannot be accessed by road or ferry. The result is that 1 out of 58 Alaskans has a pilot’s license. This high number of pilots who fly small, private aircraft, coupled with few airports, is a challenge to State law enforcement personnel, who must initially respond to crashes, render aid, locate and rescue victims, and investigate the incidents.

(See Alaska to the Appalachians, page 2)
Appalachians . . .

(Alaska to the
outlying areas has to be transported to
mote sites."

Laboratory has developed a complete
something. The Alaska State Crime

can’t go back to the office if you forget

is the ability to share fingerprint and mug shot
information as they are gathered for
systems. “Of particular importance is the
duplication of effort in keying in
data exchange system. This will avoid
the extrapolation of effort in keying in
information in each of the separate sys-
tems. “Of particular importance is the
ability to share fingerprint and mug shot
information as they are gathered for

NLECTC–Northwest will investigate
videoconferencing that may help
departments avoid the time and
expense of this travel.

Training Challenges. Because
small agencies seldom can exchange
information or host practices with
other agencies, training and sharing
information are big goals for NLECTC–
Northwest. Griffiths wants to establish
an open line of communication to en-
able Alaska agencies to share infor-
mation via the Internet. His center will
help individual agencies build their
infrastructures to allow this interaction.

Distance learning opportunities are
needed not only in Alaska. Griffiths
says they are needed by rural and
geographically isolated agencies nation-
wide. NLECTC–Northwest will be work-
 ing closely with RULETC to develop
those opportunities.

Alaska, he says, is beginning to
deploy geographic information systems
(GIS) applications for patrol officers in
rural areas to use in search and rescue
operations. State law enforcement agen-
cies also are beginning to use GIS to map
crime trends and crime rates in certain
areas. Because agencies are free law enforce-
ment officers, they need to be effective
and efficient in targeting crime. GIS crime
analysis is not yet widespread, however,

and Griffiths would like to host train-the-
trainer programs, working with the crime
mapping programs at NLECTC–Rocky
Mountain and NLECTC–Southeast, to
increase its use.

NLECTC–Northwest also is assembl-
ing an advisory council, which will be
active by spring 2002. Initially, most
members will be Alaskan law enforce-
ment and corrections officers. As the
center grows, however, Griffiths plans
to include members who have experi-
ence working with extreme weather
challenges. The center is developing a
needs assessment survey for all law
enforcement and corrections agencies
in the State. The survey will be support-
ed by research staff at the University of
Alaska’s Justice Center. By the time the
advisory council is on board, NLECTC–
Northwest should have the results of
that survey to guide its assistance to
Alaska’s law enforcement and correc-
tions agencies.

NLECTC–Northwest is hosted by the
Chenega Technology Services Cor-
poration (CTSC), a subsidiary of the
Chenega Corporation, a Native Alaskan
corporation whose stockholders live on
an island in Prince William Sound. CTSC
provides technology services, technical
support, and systems integration to
such clients as the U.S. Department
of Defense, the Defense Advanced Re-
search Projects Agency, and the Nation-
al Security Agency. CTSC is developing
distance training programs for the mili-
tary. NLECTC–Northwest will be able to
apply elements of these programs to law
enforcement and corrections needs.

For more information on the
National Law Enforcement and
Corrections Technology Center-
Northwest, contact Bob Griffiths,
866-569-2969 or 907-569-2969, or
email nlectc_nw@ctsc.net.

Technology RDF

There are more than 14,600 small
and rural law enforcement agencies with
50 or fewer officers; most have 10 or
fewer officers. These agencies represent
almost 90 percent of all law enforcement
agencies in the United States. Despite
their size and location, these smaller de-
partments face many of the same crimes
that their larger municipal counterparts
do, often without enough manpower,
training, or technology. “These are agen-
cies that can benefit mightily from the
force multiplier of technology,” says Rod
Maggard, director of the new Rural Law
Enforcement Technology Center.

“Small law enforcement and correc-
tions have been left out of access to
technology research, training, and
technical assistance that have been
granted to larger agencies,” he says.

“They’re problems are as great, if not
greater, than those faced by large
departments because they are com-
ounded by the lack of manpower,
training, technology, equipment, fund-
ing information, and information shar-
ing and capacity building.”

RULETC is unique and long overdue,
says Maggard. “Rural departments make
up the majority of United States law
enforcement agencies. They deal not
only with the same types of crimes as
their big city counterparts but also with
agricultural crimes like ecotermination,
the cultivation or manufacture of illicit
drugs in rural areas, and other crimes such
as poaching or illegal dumping.” Maggard
is well aware of the challenges small, rural
departments face. He has been in law
enforcement for 34 years, signing on as a
Kentucky State trooper in 1967, leaving in
1981 to head corporate security for Blue
Diamond Coal Company, and serving
(See Alaska to the
Appalachians, page 3)
Communication Challenges. Like their counterparts in the remote stretches of Alaska, small and rural agencies have communication problems. RULETC will concentrate on information technologies, communications, evaluations of available off-the-shelf technologies, and other technology areas that can improve the effectiveness and efficiency of rural law enforcement. “We want to bridge the information and technology gaps that exist in so many small and rural agencies,” Maggard says. His center will review technologies and best practices as they apply to the needs of rural agencies and disseminate that information to other agencies across the country.

“Communication problems are exacerbated by geographic isolation, limited interoperability, and limited equipment. Small and rural agencies simply do not have the tax base for anything other than the most essential police equipment,” Maggard says. “It’s analogous to an elderly couple living on a fixed retirement income. They may have the budgeted year in and year out with no money for new or improved technology.” In southeastern Kentucky, he says, agencies are just beginning to get a few mobile data terminals in their patrol cars. Generally, a patrol officer who needs information must radio in the request to the dispatcher, then wait until the dispatcher retrieves the information from the computer and radios it back to the officer.

Currently, RULETC staff are part of the advisory board for a statewide technology grant that was awarded to 40 counties in southeastern Kentucky to address the interoperability of 106 agencies. When completed, the interoperability project could become a national pilot program that would share best practices and lessons learned with similar agencies nationwide.

The advisory board for this project pooled knowledge from many perspectives. Police chiefs, State police, the League of Cities, sheriffs, and academics are working to solve communications difficulties created by southeastern Kentucky’s mountainous terrain and flood plains. Maggard says, “Hazard and other communities are in valleys where any construction must be above the 100-year flood mark. The interoperability project advisory board has developed a collaborative problem-solving approach that uses private, Federal, State, and local resources. The board received permission from the Public Broadcasting Corporation to use its existing towers, which were strategically located above the high water mark, for public safety communication.

Training Challenges. In fall 2002, RULETC—currently operating in satellite facilities—will open its doors in a new 36,000-square-foot, multipurpose building. The center will have access to an 800-seat, 36,000-square-foot, multipurpose building. The center will have access to video teleconferencing capabilities, CD-ROM, DVD, and video production capabilities, and GIS for crime mapping and analysis in rural areas.

For 10 years as the chief of police of Hazard from 1991 until he became director of RULETC.

**Figures are based on Recidivism of Prisoners Released in 1993, published by the Bureau of Justice Statistics (BJS) in 1999.** (NCJ 162783). A second national recidivism study was to be released in December 2001. Later this year, other agencies will follow suite. Additional data were taken from Correctional Populations in the United States, 1995, published by BJS in 1997. (NCJ 153041).
The reference library is a tool that can cut an investigator's time by 25 to 95 percent . . . .

How do you know the program you're using is not altering evidence? Ballou says, “We were aware of some of the difficulties of these imaging products—that the literature said it would do a certain thing and investigators found out later it wouldn’t, or it would but not to the extent the manufacturer claimed.

Some individual agencies tested them on their own. They made up a mock computer system, ran an imaging tool, and then went back to compare the two. That was fine; but when you think of it on a national level, you have no unbiased person or agency testing these tools.”

CTFT is designed to provide a measure of assurance in the results of investigations based on automated tools used in computer forensics examinations. These tools are used not only by law enforcement but also by government and industry to examine electronic evidence. CTFT currently covers three functional areas:

- Disk imaging tools, which copy seized disk drives.
- Write blockers, which prevent the altering or overwriting onto a seized disk.
- Analysis tools, which are used to examine information content within seized drives.

More areas will be added as funds and capabilities for testing become available.

For more information about the Computer Forensics Tool Testing project, log on to www.ctft.nist.gov or call 301-975-8425.

National Software Reference Library

The Office of Law Enforcement Standards at the National Institute of Standards and Technology (NIST), with funding from the National Institute of Justice (NIJ) and the U.S. Customs Service, has created the National Software Reference Library (NSRL). Recently established by NIST, NSRL will cut investigation time dramatically. Had the library been available nearly a decade ago when Pollitt was investigating his junior hacker, the case probably would have required 2 hours—not 2 weeks—of his time, with the computer doing all the work.

“A 10-gigabyte hard drive might have 50,000 files on it,” says Gary Fisher of NIST’s Information Technology Laboratory and project manager at NIST. “And you have to go through those files for evidence. You may be able to analyze 99 percent of the files, but still, somebody has to decide what to look at.

“Today, hard drives boast not megabytes but gigabytes of information, which would translate into several weeks of work, at a minimum, for an investigator. In addition, criminal cases involving electronic evidence base abound in the past decade. The FBI alone will investigate well over 5,000 cases this year, compared with a few hundred just 10 years ago. Other law enforcement agencies are in the same boat, investigating an increasing number of crimes involving electronic evidence that range from fraud and hacking to drug crime and child pornography. Investigators, however, are getting some new tools to help them keep pace.

The NSRL Reference Data Set database is available on CD-ROM through NIST’s Standard Reference Data Program. There is an annual $90 subscription fee. For more information, log on to www.nsrl.nist.gov or call 301-975-8425.

Computer Forensics Tool Testing

The Computer Forensics Tool Testing (CTFT) project is a NIST/NIJ initiative that also will benefit computer crime investigators. CTFT helps determine the accuracy of computer forensics tools used to investigate or examine information found on seized computers.

According to Susan Ballou, program manager for forensic sciences at NIST, investigators use “imaging” tools to duplicate a disk drive, thereby enabling them to look for evidence on the “copy” without destroying or altering the original. As the number of these computer forensics tools proliferated in the late 1990s, however, defense attorneys, juries, and the courts began to focus more attention on this technology’s accuracy and its part in investigation, evidence collection, and prosecution.

For more information or to register, call 888-306-5382. To register online, log on to www.olec.org.

Mock Prison Riot

May 5–9, 2002
Former West Virginia State Penitentiary in Moundsville, West Virginia

Sponsored by the National Institute of Justice’s Office of Law Enforcement Technology Commercialization, the annual Mock Prison Riot offers hands-on training in the form of realistic scenarios involving inmate uprisings, hostage situations, and cellblock takeovers. The Mock Prison Riot also showcases new and developing law enforcement and corrections technologies that are incorporated into the training scenarios, field demonstrations, and exhibits.

For more information or to register, call 888-306-5382. To register online, log on to www.olec.org.
Immediately following the terrorist acts of September 11, the New York State Emergency Management Office asked the National Institute of Justice (NIJ) to provide onsite technology assistance. Within 24 hours, staff at NIJ's Office of Science and Technology had established a technology support office adjacent to the WTC complex to help coordinate technology assistance activities with search and rescue officials. Two technical representatives from NIJ staffed the technology support office during the initial search, rescue, and recovery operations.

“We were asked onsite for two reasons,” says Chris Tillery, Senior Program Manager of NIJ’s Critical Incident Technology Program and one of the first technical representatives at the WTC. “We were there to help identify the technology requirements of the Federal Emergency Management Agency’s Urban Search and Rescue (US&R) teams and the New York City Fire Department (FDNY), and to work with them in developing solutions.

“Because of the enormity of the task that lay before search and rescue personnel, it was essential that all of our resources came into play. Through NIJ’s National Law Enforcement and Corrections Technology Center (NLECTC) system and its technical partners, our onsite technical support team was able to leverage technical resources, equipment, and expertise to deliver technology that was rugged and dependable enough to assist the search and rescue teams and fire department.”

The first team to arrive in support of the technical support office was from the NIJ-funded Savannah River Technology Center (SRTC) at the U.S. Department of Energy’s (DOE’s) Savannah River Site near Aiken, South Carolina. The team consisted of electrical and mechanical engineers, a chemist, and a technician. They brought more than $500,000 worth of equipment that included cameras, microphones, crawlers, boroscopes, and other tools that could reach into inaccessible and hazardous spaces in the voids under the rubble. The SRTC team and NIJ staff provided onsite technology expertise and made real-time engineering modifications and repairs to equipment to fit specific US&R needs as they arose. To aid FDNY in detecting, documenting, and recording victims trapped and human remains found during cleanup, NIJ set up a perimeter surveillance system and trained firefighters in its use.

The next teams to arrive to help the technical support office were from the Center for Civil Force Protection, which is funded by NIJ and located at DOE’s Sandia National Laboratories (SNL) near Albuquerque, New Mexico; and from Pennsylvania State University’s (PSU’s) Applied Research Laboratory. SNL engineers had developed surveillance systems for search dogs that allow their handlers to see what the dogs see in areas where humans cannot go. The representatives from PSU provided expertise in advance acoustic technologies and terrain assessment.

On September 11, 2001, at 8:46 a.m., American Airlines flight 11, hijacked by terrorists out of Boston’s Logan International Airport, crashed into the North Tower of New York City’s World Trade Center (WTC). Sixteen minutes later, onlookers and television crews watched as terrorists crashed a second plane, United Airlines flight 175, also out of Boston, into the middle of the WTC’s South Tower. Police officers, firefighters, rescue workers, and thousands of others trying to evacuate the burning buildings were trapped when the 110-story South Tower suddenly collapsed at 9:59 a.m. At 10:28 a.m., the 110-story North Tower also collapsed, burying and eventually destroying five other buildings and the nine below-ground levels of the WTC complex. Almost 3,000 people, including rescue workers, were killed.

According to engineers interviewed by the media, each tower was built around a central steel core surrounded by open office space. Supporting 18-inch steel tubes ran vertically along the outside of the buildings. When the planes damaged the central cores, the weight of the buildings was redistributed to the outer steel tubes, which buckled under the added weight and the intense heat of the fires. The resulting debris pile was five stories high.

As the attacks unfolded in New York City, terrorists hijacked another plane out of Dulles International Airport in northern Virginia, near Washington, D.C. At 9:40 a.m., this plane, American Airlines flight 77, crashed into the west side of the Pentagon. Shortly thereafter, reports of another hijacking began to filter in. At 10:10 a.m., United Airlines flight 93 out of Newark International Airport in New Jersey crashed in Stonycreek Township in rural Somerset County, Pennsylvania, killing all aboard. Experts believe the plane was heading for another high-visibility target, possibly the U.S. Capitol or the White House.
and delivery of more than $850,000 worth of equipment available through its 1033 Program. In addition, staff from NIJ’s Investigative and Forensic Sciences Division and the NLECTC system began identifying forensic and investigative assistance resources. The Federal Laboratory Consortium (FLC) for Technology Transfer also helped identify technologies that could aid in the WTC search, rescue, and recovery mission. The FLC rapidly disseminated information to more than 700 Federal laboratories and centers. Numerous facilities offered to help with technology and expertise. The operational challenges and hazardous working conditions faced by the urban search and rescue teams limited the practical use of many technologies,” according to Joe Cecconi, an NIJ Program Manager with an engineering background who also went to the WTC site. “However, groundwork was established for future partnerships.” He says that since the WTC attack, NIJ has continued to provide technology information, assistance, and expertise to the public safety community in the areas of critical incident planning and response.

“As a result of the events of September 11, we have received many valuable recommendations from the responding agencies and departments in terms of new technology research and development and in modifying existing technologies.”

**Search and Rescue Assistance**

**Canine Camera.** On September 20 at the WTC site, the Florida US&R team used the first of six canine cameras. The cameras provided views of remote areas that dogs could access but humans could not. SNL developed these canine cameras and modified them onsite. Lighting was added so the dogs could search in dark areas. In addition, an audio control allowed handlers to give commands to their dogs. The California US&R team also deployed the canine cameras.

**Pole Camera.** The NII team fabricated a pole camera to replace one that had been broken during an earlier search and rescue effort. During a debriefing, the team recommended changes to enhance the pole camera’s design and performance and advised that commercial versions are also available.

**Void-Search or Drop Camera.** Search and rescue teams used the void-search or drop camera to explore several voids in the rubble, stairs, and an underground parking lot. The Pennsylvania and Texas US&R teams used a makeshift drop camera assembled from a commercial technology primarily intended for deployment-tethered mobile robots. SRC engineers converted an underwater pan/tilt/zoom/lights camera assembly into a portable unit for vertical deployment into 100-foot voids. Although the temperatures in some of these voids were estimated to be 1,000 degrees Fahrenheit, the camera performance was unaffected.

**Perimeter Surveillance.** At the request of FDNY, NIJ staff developed a system of cameras for perimeter surveillance of the WTC site. With technical and manpower assistance from the Nassau County (New York) Police Department, NIJ staff and SRC engineers set up six strategically placed cameras that allowed searchers to remotely monitor sites, identify areas with potential victims, and send in appropriate response teams.

**Thermal Imaging.** NIJ made available thermal imagers and trained US&R teams in their use. Thermal imagers “see” what are essentially differences in temperature—differences as small as 1 degree. They can show the location of anything that retains heat, such as a living person.

**Communications and Interoperability Assistance**

**AC11–1000.** NIJ’s AGILE program is evaluating an AC11–1000 communications switch at the Alexandria, Virginia, Police Department. This switch provides communications interoperability during critical incidents by linking voice communications among disparate radio systems, thereby enabling different agencies and jurisdictions to communicate with each other. Following the September 11 attack on the Pentagon, the AC11–1000 was activated and partner agencies were advised that the AC11–1000 was available. (Partner agencies include the FBI, the Secret Service, and the U.S. Park, U.S. Capitol, the Metropolitan D.C., Metro Transit, Maryland State, Virginia State, Arlington, and Alexandria Police Departments.) A number of active channels were monitored, which enabled AC11–1000 testbed personnel to provide dispatchers with information from other departments, direct radio links between the partner agencies were not requested. The testbed personnel provided communication support throughout the response to the Pentagon attack and remained ready to provide direct radio links between the responding agencies. They also completed the FBI’s request to program a new frequency in the AC11–1000 for their Washington field office communications.

**Mobile and Voice Data Communications.** The New York State Emergency Management Office requested communications assistance from NLECTC–Northeast employees who work for the New York State Technology Enterprise Corporation (NYSTEC), a technology adviser to the New York State government. By 10 a.m. on September 11, NYSTEC had mobilized a state-of-the-art mobile and voice data communications center to help the State quickly set up military communications throughout New York City and to reestablish the critical data lines that connect Albany to numerous State facilities throughout the city.

**Excess Property and Equipment Assistance**

**1033 Program.** NLECTC–Northeast coordinated a systemswide effort to send excess boots, clothing, protective and work gloves, ropes, gas masks, ballistic-resistant helmets, laptop computers, and other needed equipment to rescuers. The equipment was secured through the Georgia 1033 Coordinator’s Office and the U.S. Department of Defense’s Defense Reutilization Marketing Office in Fort Jackson, South Carolina. The Charlotte (North Carolina) Police Department and other law enforcement agencies provided a police escort for the trucks that transported the equipment.

**Refrigerated Storage.** In response to a request from the New York State Police, NLECTC identified and arranged the delivery of two walk-in portable and four semi-truck mobile refrigerated units for storage of DNA samples from the WTC site at the New York State Police Forensic Investigation Center.

**Investigative and Forensic Assistance**

**Audio Technologies.** At the request of the New York County (Manhattan) District Attorney’s Office, NLECTC–Northeast’s Law Enforcement Analysis Facility (LEAF) staff prepared numerous audio technologies for possible use. These included a speaker identification program that can identify a person from as little as one word of speech and a speech enhancement program that can reduce noise or interference from a variety of media without distorting the words. LEAF staff processed an audiotape that contained Arabic using the Air Force Research Laboratory’s speech enhancement technologies. Once the processing was completed, the tape was returned to the District Attorney’s Office for further investigation.

**DNA Analysis.** NIJ offered hardware and software assistance to the Armed Forces DNA Identification Laboratory and the New York City and State crime laboratories. These labs are using forensic DNA testing to identify victims of the September 11 attacks.

NIJ further expanded the Kinship and Data Analysis Panel of renown experts in the areas of parentage testing, genetics, genomics, information technologies, bioinformaticians, and other related disciplines in the field. The panel has been highly involved in recommending and developing protocols, methodologies, and analytical support for the mass identification project being undertaken at the WTC site.

**Other Assistance**

**New York Electronic Crimes Task Force.** The U.S. Secret Service New York field office and the New York Electronic Crimes Task Force (NYECTF) office were in Building 7 of the WTC, which was destroyed. Fortunately, the entire staff survived, but all records, computers, and software tools were lost. NLECTC–Northeast assisted NYECTF in acquiring new computers, software, and such office equipment as fax machines and safes.

**Odor Perception Inhibitor.** The Office of Law Enforcement Technology Commercialization (OELTC) in Wheeling, West Virginia, arranged for thousands of vendor-donated odor perception inhibitor packets for search and rescue workers. Putex (formerly known as Carry-On) is a gel-based inhibitor that isolates and eliminates patrascene and cadaverine, two compounds associated with decomposing or burnt flesh. The product, however, does not inhibit other odors, such as natural gas, that could signal an environmental hazard. OELTC had assisted in the commercialization of this product in early 2001.
No matter what the critical incident, first responders face similar problems: less than total response coordination across jurisdictions and among agencies, lack of training, and equipment deficiencies.

No matter what the critical incident, efficient and effective partnerships—partnerships among agencies at critical incident size as well as partnerships for providing training, developing new technologies, and exploring ways to prevent terrorism and other criminal acts.

No matter what the critical incident, without a unified, coordinated response that uses advanced equipment and technologies, lives will be lost, time will be wasted, and resources will be underutilized.

In 1997, the National Institute of Justice (NIJ), through its Office of Science and Technology (OST), initiated a critical incident technology program to develop solutions relating to agency coordination, personnel training, and equipment and technology development. This program is a collaborative effort among Federal, State, and local public safety agencies.

This multidisciplinary, multiagency approach extends NIJ’s objective of preparing law enforcement and public safety communities to respond to terrorist incidents by building on existing capabilities for handling other emergencies.

“What is important to understand about NIJ’s critical incident technology program is that we don’t just look at the needs of law enforcement, we focus on problems common to all public safety agencies,” says Chris Tillery, the Senior Program Manager for NIJ’s Critical Incident Technology Program.

“Coordinating a combined response among agencies from multiple jurisdictions is difficult during any critical incident, whether it’s a terrorist attack, a natural disaster, or an industrial accident. But through these partnerships, NIJ identifies gaps in existing technology efforts and leverages its $10 million annual investment with investments from other agencies that total hundreds of millions of dollars. Since its inception in 1997, this collaborative effort has already produced a number of new technologies. Some already are in use, and some are still in the testing stage.”

Biohazard and Chemical Defense

• The Office of Law Enforcement Standards (OLES) at the National Institute of Standards and Technology coordinates the development of standards for chemical and biological protective equipment for responders. OLES, which is funded by NIJ, collaborates with the Technical Support Working Group (TSWG), a joint effort of Departments of Defense, State, Justice, and Energy; the FBI’s National Domestic Preparedness Office; the National Forensic DNA Analysis Center; and the Centers for Disease Control and Prevention.

• NIJ’s AGILE program addresses communications interoperability and information sharing issues that result when agencies from multiple jurisdictions respond to a critical incident. Both short-term and long-term interoperability solutions are being developed for wireless telecommunications and information sharing technology based on three major program elements: (1) standards; (2) research, development, test, and evaluation; and (3) outreach. Through this approach, AGILE aims to raise the awareness of interoperability issues and disseminate short, best practices learned, and best practices so that policymakers and public safety leaders can make informed, cost-effective decisions.

• INFOTECH uses existing systems and networks to promote information sharing among law enforcement agencies. It is fully operational in two Florida county sheriff’s offices and is in the implementation stages in California, Oregon, and Virginia. The system, created in cooperation with the U.S. Navy Space and Naval Warfare Systems Center (SPAWAR) in Charleston, South Carolina, expands on technology originally developed by the U.S. Department of Defense’s Joint Program Office for Domestic Preparedness.

• NIJ is in the initial stages of implementing a chemical detection system for real-time early warning, chemical and biological detection and emergency alarm systems for subways.

• NIJ, in collaboration with the U.S. Army Research and Development Division, the Institute for Security Technology Studies at Dartmouth College, and SPAWAR–Charleston, is developing the technology.

• NIJ, through TSWG, conducted a study to identify practitioner requirements for bomb robots. A solicitation for development of a robot that would meet these requirements was released in 2001.

Explosives Detection and Remediation

• Operation America is an advanced training opportunity for bomb technicians. This event features examples of the latest technologies that a bomber could use to construct a complex, hard-to-defeat device. Techniques include advanced initiation sequences, antiterrorist mechanisms, and booby traps. Personnel from SNL demonstrate the latest technology and approaches to render safe such advanced devices.

• Through JPDG, NIJ is working with TSWG to develop a protective mask that would give responders time to exit a hazardous area, alert the proper officials, and stop others from entering the area. The mask, which is intended for use in situations where authorities receive little or no warning, needs to be lightweight, easily carried and used, and inexpensive. It also could be used to protect victims during evacuation.

Communications and Interoperability

• NIJ’s AGILE program addresses communications interoperability and information sharing issues that result when agencies from multiple jurisdictions respond to a critical incident. Both short-term and long-term interoperability solutions are being developed for wireless telecommunications and information sharing technology based on three major program elements: (1) standards; (2) research, development, test, and evaluation; and (3) outreach. Through this approach, AGILE aims to raise the awareness of interoperability issues and disseminate short, best practices learned, and best practices so that policymakers and public safety leaders can make informed, cost-effective decisions.

• INFOTECH uses existing systems and networks to promote information sharing among law enforcement agencies. It is fully operational in two Florida county sheriff’s offices and is in the implementation stages in California, Oregon, and Virginia. The system, created in cooperation with the U.S. Navy Space and Naval Warfare Systems Center (SPAWAR) in Charleston, South Carolina, expands on technology originally developed by the U.S. Department of Defense’s Joint Program Office for Domestic Preparedness.

• NIJ is in the initial stages of implementing a chemical detection system for real-time early warning, chemical and biological detection and emergency alarm systems for subways.

• NIJ, in collaboration with the U.S. Army Research and Development Division, the Institute for Security Technology Studies at Dartmouth College, and SPAWAR–Charleston, is developing the technology.

• NIJ, through TSWG, conducted a study to identify practitioner requirements for bomb robots. A solicitation for development of a robot that would meet these requirements was released in 2001.
Counterterrorism Institutes

There are terrorist entities inside and outside of our Nation that, for whatever reasons, would try to harm America’s citizens, security, and prosperity. To respond effectively to terrorist attacks and identify, investigate, and pursue the attackers, substantial research, technology development, and organizational efforts are required.

Two resources of information and research available to State and local law enforcement are the Institute for Security Technology Studies and the Oklahoma City National Memorial Institute for the Prevention of Terrorism, both sponsored by the National Institute of Justice (NIJ).

Institute for Security Technology Studies

The Institute for Security Technology Studies at New Hampshire’s Dartmouth College focuses its research, development, and assessment efforts on countering terrorist attacks on websites and other Internet components and protecting the integrity of infrastructure systems such as networks. Funded under a grant from NIJ’s Office of Science and Technology, the Institute and its core research program assess threats against the Nation’s electronic information infrastructure technologies and systems. This core program evaluates potential techniques and technologies designed to prevent cyberattacks and maintain infrastructure integrity. By assessing current developments in the field, the Institute also helps define a national research agenda on cyberterrorism.

Oklahoma City National Memorial Institute for the Prevention of Terrorism

The efforts of the Oklahoma City National Memorial Institute for the Prevention of Terrorism (MIPT) target the activities of individuals who are on a watch list. This Institute, sponsored by the National Institute of Justice (NIJ), sponsors research on equipment, training, and procedures aimed at helping police officers, firefighters, emergency medical technicians, and others who are first on the scene of a terrorist incident. Originally incorporated as a nonprofit organization in the aftermath of the 1995 bombing of the Murrah Federal Building, MIPT’s mission is to prevent acts of terrorism and subsequent suffering throughout the Nation. MIPT’s five core program areas are research and development, outreach and education, training, response coordination, and lessons learned.

Although both institutes have their areas of specialization, they also conduct and sponsor research into other aspects of counterterrorism. To find out more about the Institute for Security Technology Studies, visit www.ists.dartmouth.edu or contact Paul Gnon at 603–646–0700. For more information on the Oklahoma City National Memorial Institute for the Prevention of Terrorism, visit www.mipt.org or contact Brian Houghton at 405–278–4311.

Special Report

Counterterrorism

In partnership with, cont. from page 7

JUSTNET at www.justnet.org.

Video. NIJ is working with the FAA to explore the possibility of placing a portal at New York City high school. The FAA has a portal currently in use in the Bannock County, Idaho, courthouse and in a New York City high school. The FAA has a portal under evaluation. The portal was commercialized in 2000 by Quantum Magnetics and Milestone Technologies as the SecureScan 2000.

Other initiatives

The NIJ-funded Center for Civil Force Protection offers assistance to State and local law enforcement agencies and other public safety agencies on combating terrorism and responding to other critical incidents. Information and assistance are available in such areas as architectural safety, biometrics, bomb suits, and vulnerability analyses.

Other NIJ partners in the Critical Incident Technology Program include the Centers for Disease Control and Prevention, Eastern Kentucky University, the InterAgency Board for Equipment Standardization and InterOperability, the Oklahoma City National Memorial Institute for the Prevention of Terrorism, and the OJP Office for Domestic Preparedness.

For additional information, visit the NLECTC Virtual Library page on JUSTNET at www.justnet.org.
The following list can assist public safety personnel in finding information and training resources in their efforts to prevent terrorist attacks and respond to them should they occur.

Chemical/Technical Defense

Publications


Websites
- Center for Civilian Biodefense Strategies, Johns Hopkins University: http://www.hopkins-biodefense.org

Chern-Bio: www.chern-bio.com

National Institute for Occupational Safety and Health, Centers for Disease Control and Prevention: www.cdc.gov/niosh/homepage.html

Cybercrime

Publications


Websites

- Department of Computer Forensics, Washington University: www.dcfw.net

- Internet Fraud Complaint Center, Federal Bureau of Investigation and National White Collar Crime Center: www.ifcc.gov

- National Center for Forensic Science: ncf.sfsu.edu

- Cyber Crime Training Partnership: www.nictp.org

- National Law Enforcement Cybercrime Laboratory: www.nlcic.gov/elm/elmcenter.html

- National White Collar Crime Center: www.nwc3.org

- www.cybercrime.org

Explosives Detection and Remediation

Publications


Infrastructure/Physical Security

Publications


- Videos

Websites
- National Infrastructure Protection Center: www.nipc.gov

- U.S. Department of Energy: www.energy.gov

- National Telecommunications and Information Administration, U.S. Department of Commerce: www.ntia.doc.gov

General Resources

Publications


- Videos


- Websites for Federal Government Institutions, Organizations, and Programs

- Bureau of Alcohol, Tobacco and Firearms: www.atf.treas.gov

- Centers for Disease Control and Prevention: www.cdc.gov


- Federal Bureau of Investigation: www.fbi.gov


- Preparatory Training & Exercises: www.fema.gov/jtr


- National Criminal Justice Reference Service: www.ncjrs.org


How to order publications and videos
Each publication and video entry includes a colored square indicating that it is available from either the National Criminal Justice Reference Service (NCJRS) or the National Law Enforcement and Corrections Technology Center (NLETCC). Publications and videos that have a • may be ordered by calling 800–651–2482; many NCJRS publications may also be downloaded from the Justice Information Center at www.ncjrs.org. Publications and videos that have a ^ may be requested by calling 800–248–2742. These publications can be downloaded from JUSTINET at www.justinet.org.

How to find information at Internet sites
Because the content and organization of websites change fairly often, the addresses or URLs listed will most often take users to the top-level home page of the site. In general, to find more specific information, users will have three options: (1) explore the site using the navigation buttons available on the home page, (2) search the site using its search engine (usually a link from or button on the home page), or (3) look through a URLS listed will most often take users to the top-level home page of the site. In gener-

| Special Report | Counterterrorism |

9

01-TechBeat Winter 2002 1/24/02 3:04 PM Page 9

If You Need More Information . . .
Technology can significantly enhance the effectiveness and efficiency of law enforcement, corrections, and forensic sciences. Just as important, it can help protect 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:

- Standards and Testing/Technology
- Technology Assistance
- Technology Identification
- Technology Needs Assessment/ Prioritization

Technology Demonstration
NLECTC assists and demonstrates new and emerging technologies through such special events, conferences, and demonstrations as the Black Hawk Ride (Technologies for corrections), Operation America (body 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.

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

Technology Information Dissemination
NLECTC disseminates information to the criminal justice community at no cost through the online database, seminars, equipment performance reports, guides, consumer product evaluations, meeting/conference reports, videotapes, and CB/BBMAs. NLECTC also publishes Technology; an award-winning quarterly newsletter. Most publications are available in electronic form through the Justice Technology Information Network (JTINET) at www.jtinet.org. Hard copies of all publications can be ordered through NLECTC’s toll-free number, 800–249–2972, or via e-mail at nlectc@nlectc.org.

NLECTC – National
21775 Highway 118
Rockville, MD 20850
800–249–2742
asknlectc@nlectc.org

NLECTC – Northeast
20 Electronic Parkway
Rivermont, NJ 08141–6114
888–336–0584
nlectc_ne@nlectc.org

NLECTC – Southeast
5100 International Boulevard
North Charleston, SC 29418
800–292–4385
nlectc_se@nlectc-se.org

NLECTC – Rocky Mountain
2050 E Iliff Avenue
Denver, CO 80208
800–416–8086
nlectc-rm@dod.gov

NLECTC – Northwest
4900 Cstial Sevenar Highway, Suite 301
Anchorage, AK 99501–5050
866–560–2969
nlectc_nw@nlectc.net

Border Research and Technology Center (BRTC)
1002 Second Avenue, Suite 1120
San Diego, CA 92101–4912
888–606–1783
oles@nist.gov

Office of Law Enforcement Technology Commercialization (OLETC)
2050 E Iliff Avenue
Denver, CO 80208
800–292–4385
nlectc_ne@rl.af.mil

Office of Law Enforcement Technology Commercialization (OLETC)
2001 Main Street, Suite 500
Rockville, MD 20850
888–306–5382
oletc@oletc.gov

Office of Law Enforcement Standards (OLES)
150 Bureau Drive, Suite 150
Gresham, OR 97030–7125
866–787–2555
nlectc@doj.org

Technology Identification
As an agency’s first step in its search for new and developing technologies, NLECTC provides information relating to availability, performance, durability, reliability, safety, ease of use, customer satisfaction, 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 offer years of experience in engineering. Areas of assistance include evidence analysis (e.g., audio, video, computer, trace, and explosives), systems engineering, and communication 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 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 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 rifles, 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 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.

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.
In addition to funding the National Law Enforcement and Corrections Technology Center, 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.

In addition, 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; www.ncjrs.org.
All About TechBeat

TechBeat is the award-winning flagship publication 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 Editors/ Writers, Gayle Parraway and Lois Pilant; Contributing Writers, Nyla Mouser, Becky Lewis, and Jackie Siegel; Editor, Michele Coppola; Graphic Designers, C. Denise Collins and Tina Kramer.

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 newsletter 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 2001 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.


www.justnet.org

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.

Interactive Topic Boards: that allow you to post questions and exchange information with hundreds of professionals in their specialty areas.

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.

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.
TechShorts 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 newsletter reproduces synopses of recent articles relating to technology developments and initiatives in law enforcement, corrections, and the forensic sciences that have appeared in newspapers, newsmagazines, and trade and professional journals. The summaries are also available through an electronic e-mail list, JUSTNETNews. Each week, subscribers to JUSTNET-News 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 2001, Information Inc., Bethesda, Maryland.

Life or Meth

Law Enforcement Technology

Because of their hazardous and volatile natures, chemicals used in making methamphetamine (meth), law enforcement agents and emergency personnel risk injury from inhalation or contact, or even fire or explosion, when they happen upon a meth lab. According to data compiled by the Agency for Toxic Substances and Disease Registry, meth labs numbered 11,513 in 1998 and are up 18% for the year 2000. Fortunately, the police officers who were the first to respond, 8 firefighters, and 3 paramedics who assisted, were unharmed. Methamphetamine is created through a heating or chemical process, and the “recipe” can be found on the Internet. Because not much equipment is needed to cook meth, labs often are hidden in vehicles, allowing makers to avoid detection by moving around constantly. A strong odor resembling cat urine often is a giveaway for a lab, but if noticed by a police officer, it means that contaminants are in the area and the officer should leave immediately without touching anything. Officers should be particularly careful not to discharge their firearms or turn on lights because both actions could trigger an explosion. A coordinated effort between the police department, the local fire department, and emergency medical services should be employed to reach a meth lab, andgoritms suit. Scales, and nitroglides should be used to avoid contamination.

Antithete Site Excels With Speed, Accuracy

USA Today

The Anti-Displacement League (ADL) is helping law enforcement agents combat hate crimes by launching a website that serves as an “instant resource” for hate crime information. The site features information about different hate groups and a calendar of events related to planned extremist activities. Anyone may visit the site. Law enforcement groups have confidence in the integrity of the information provided by ADL, says Douglas Scheurer, vice president of the New Jersey Association of Chiefs of Police. The ADL site is published weekly as part of the National Law Enforcement and Corrections Technology News Summary.

Sounding Out Snipers

Scientific American

The Defense Advanced Research Projects Agency is preparing law enforcement agencies for urban warfare by commissioning prototypes of specialized technologies. BBN Technologies, a division of Verisium, has designed a sniper-detection device that will allow soldiers to track the direction of a bullet back to a hidden enemy, which can then be transmitted to a global position system. The new battlefield technology will use microphones and a helmet-mounted compound. The device also can be mounted on trucks, airplanes, streetlights, and buildings. BBN’s technology tracks snipers at long distance by picking up the acoustic vibrations from the muzzle blast and the supersonic crack of the bullet. The technology also is able to detect the trajectory, caliber, and speed of the bullet.

We All Leave High-Tech Fingerprints

Austin American-Statesman

Computer forensic specialists can look at a disk drive and learn everything from passwords to a sequence of keystrokes to what was written in an email sent years ago. Law enforcement officers say that by hitting delete, they have successfully erased data from a terminal, but computers were designed to remember things. The U.S. Department of Defense drilled holes in its drives to get rid of information, and many private companies rely on new software that effectively erases a user’s history from a computer. A Texas company offers individuals the chance to erase their drives, but at the same time, its employees use its services to create a profile of a worker’s computer when he has left a company to check for trade secret violations and economic espionage.

Teens Can Get Fake IDs in a Few Keystrokes on Web

Christian Science Monitor

The Internet is making it easy for teenagers to procure fake IDs, according to high school owners and U.S. law enforcement agencies. The holograms and encoding technologies found on real IDs have thus far proved effective at minimizing identity theft and forgery. Meanwhile, the number of websites dedicated to creating fake IDs continues to rise, and inexpensive Internet templates and other forms of technology are only adding to the problem. ID forgery has skyrocketed, and the FBI is greatly outmatched in its fight to combat the problem, says Dallas-based security expert Dana Tierney. Prosecutions in these cases are few and far between.

Cameras To Monitor Border

San Antonio Express-News

Operation Rio Grande will involve the placement of high-tech infrared cameras on towers along 29 miles of the state to monitor illegal crossings of the U.S.-Mexico border. Jaime Salazar, a spokesman for the Border Patrol, notes that fewer agents will be necessary to guard the border and that agents will now be able to move instead of staying in one place. Images from the cameras, which have a range of 3 miles during the day and 1.5 miles at night, will be relayed to a station in Brownsville, Texas. The U.S. Coast Guard, U.S. Fish and Wildlife Service, and U.S. Customs Service will also make use of the cameras. The Brownsville area has been waiting since 1997 for the cameras to put in place. Installation was delayed because environmental activists complained that endangered species could be threatened by Operation Rio Grande.

Inmates Face Eye Test for Drugs

Toronto Star

Ontario, Canada, will begin using technology developed by a Maryland-based company on its inmate population to test if prisoners are under the influence of contraband drugs or alcohol. Instead of taking a urine test, inmates simply have to look into a special retina finder that reveals whether they are currently on any illicit substance. The system is being introduced in advance of new random drug testing policies that will go into effect in 2000.

Bioinformatics at Work?

InfoWorld

Recent progress in biometrics—the electronic storage and scanning of people’s unique physical makeup—is making the security technique more affordable, accurate, and scalable. The least costly and simplest biometric application is fingerprint scanning. Although fingerprint scanning is the most common technique employed by companies, hand geometry is more reliable. Voice verification is also a viable option, although the difference in telephone handsets and line quality limits its effectiveness in internal networks. Entities with great security needs often employ the more expensive options of iris scans, retinal imaging, and facial recognition. Verification systems carry lower price tags, are quicker, and produce fewer false positives than identification systems. An important consideration in choosing a verification system is whether to store the users’ characteristics locally or in a central database. Local storage inhibits users from moving to a different machine, while centralized databases’ disadvantages are greater security threats and the large amount of traffic.

Problem Drivers on a Short Leash

Civic.com

Suspended drivers may be forced to wear a new wireless device on their wrists after conviction. The device bears a coded signal to police cars that have a special antenna and a mobile computer. The system was created as part of an initiative by the National Highway Traffic Safety Administration and is being tested by police in Norwalk, Connecticut. According to officials, the Problem Driver Detection System will alert law enforcement when a restricted driver is operating a vehicle by picking the signal from within the police vehicle when it is within about a quarter-mile. System designers hope to develop a global positioning system function in the future, allowing officers to locate the exact area of the transmitter. In addition, the system will be mostly funded by the offenders, while law enforcement agencies will be responsible for the antenna cost.
Maple Street
24
Elm Street
33rd Avenue
34th Street
First Street
Birch Street
Innovative Technologies for Community Corrections Conference
May 20–22, 2002
San Diego Marriott Mission Valley • San Diego, California

■ Non-Invasive Drug Testing
■ Automated Reporting Systems
■ Supervising High-Tech Offenders
■ Fugitive Apprehension Technologies
■ Technology for Managing Sex Offenders
■ Distance Learning and Computer-Based Training
■ Management Issues in Implementing Technology
■ Advances in Electronic Monitoring
■ Crime Mapping for Community Corrections
■ Mobile Computing
■ Case Management Systems

Registration fee:
$100 per person (covers the cost of meals)

The conference will spotlight the innovative use of technology in community corrections and provide a glimpse of the technologies in development that will soon be available to assist agencies with their mission performance.

Tentative topics include:
For more information or to be placed on our mailing list for information regarding this conference, please call Jennifer Dunne at 800–416–8086, or e-mail jdunne@du.edu.

Hosted by the National Law Enforcement and Corrections Technology Center–Rocky Mountain, a program of the National Institute of Justice

For more information about the Rural Law Enforcement Technology Center, contact Rod Maggard, 606–436–8848, or e-mail ruletc@aol.com.

National Law Enforcement and Corrections Technology Center
P.O. Box 1160
Rockville, MD 20849–1160

Maggard says that because RULETC represents all small and rural agencies throughout the United States, its advisory council will include representatives from departments and agencies across the country. Maggard already is collaborating with the other NLECTC facilities to identify law enforcement professionals who are familiar with the challenges of law enforcement on a small scale and who have specialized knowledge in the center’s focus areas.

RULETC’s host agency is the Eastern Kentucky University Justice and Safety Center, a component of the College of Justice and Safety, which is involved in numerous Federal, State, and local projects. The Justice and Safety Center focuses on law enforcement technology, crime prevention, domestic violence, and community-oriented policing. Working with the National Institute of Justice’s Office of Science and Technology, Eastern Kentucky University has developed distance learning and computer-based training on such topics as weapons of mass destruction, DNA evidence collection, Spanish for law enforcement, and school security evaluations. RULETC will collaborate with other universities to enhance distance learning and offer teleconferencing training opportunities across the country.

As part of the development of RULETC, the Justice and Safety Center created a needs assessment survey that was mailed out nationwide. The self-report survey included both closed- and open-ended questions on the use of technology in small and rural departments. “We wanted to learn the types of technology these agencies currently use and how frequently they use it, their technological needs, their attitudes toward technology, the availability of technology training, and their organizational demographics,” Maggard says. A research report based on the survey and on the advisory council’s recommendations will help RULETC to build a responsive rural law enforcement program.

For more information about the Rural Law Enforcement Technology Center, contact Rod Maggard, 606–436–8848, or e-mail ruletc@aol.com.