Getting a ‘TIP,’ Making a ‘Linc’

From following up on a report of a missing child to responding to suspected acts of terrorism, rapid access to current information is crucial to public safety agencies. Unfortunately, that information usually resides in stand-alone databases of individual agencies, making it difficult for neighboring jurisdictions to obtain, if at all. There is no one-size-fits-all solution to information access and management. However, a number of local-level initiatives across the Nation are proving to be effective. Two of these initiatives are the Intelligent Linked Information Networked Collaboration System (iLincs) in Ohio and the Low Country Information Technology Improvement Project (ITIP) in South Carolina. While aimed at different types of information sharing, they do have two elements in common. Both use the Global Justice eXtensible Markup Language Data Model (see page 2) and both are receiving assistance from the National Institute of Justice’s (NIJ’s) National Law Enforcement and Corrections Technology Center (NECTC) system.

About iLincs

An officer responding to a call about a missing child uses a digital camera to capture a picture of a photo provided by her mother. From his patrol car, he creates a missing child record and uploads the image; an alert appears on the agency’s missing children “hot list.” Through personal computers in their cruisers, all department officers now have access to the child’s picture. Fortunately, 2 hours later, she is located by an officer at a nearby mall, and all other officers who received the alert are instantly notified that she has been found.

Officers from eight Ohio law enforcement agencies now can instantly share field intelligence reports, photos, mug shots, and fingerprints through the Intelligent Linked Information Networked Collaboration System (iLincs). This Web-based tool accesses, captures, and shares images and information through personal computers in patrol cars. iLincs consists of software applications, hardware, and support that provide agencies with the capability to share photos, FBI reports, and access to multiple crimefighting databases; to electronically scan and match fingerprints; and to access and serve warrants.

Developed by the Ohio-based Armada Group, Inc., iLincs uses industry standard technology and requires a PC-based laptop, desktop, or mobile data terminal with two USB ports, running Microsoft® Windows® 2000 or XP Professional and Internet Explorer 6.0 or higher. Participating agencies need only computers and Internet connections to make it work. The secure Web-based subscription service does not require capital expenditures for software or hardware, training for technical personnel, a lengthy timeframe for installation, or maintenance and upgrade fees.

The instant access to information and photos that iLincs provides not only allows officers to respond to crises more quickly and efficiently—it also helps them perform their everyday duties better by allowing quicker identification of suspects and fugitives. It can even alert them to the possible dangers of a confrontation that may result from a routine traffic stop.

“I was a street cop for 13 years,” says Armada founder Keith Singleton, a former officer with the Columbus Division of Police. “In 1987, I carried a stack of 3 by 5 FI [field interview] cards. I was frustrated in the field, sometimes having to let the wrong people go because I didn’t have good identification. What we needed were mug shots in the cruiser.”

Singleton envisioned automating the process. “Imagine stopping a vehicle, doing a license plate search, and getting a full report immediately with photos and prints.

No More ‘Cell’ Phones

In the late-night quiet of a prison cellblock, an inmate slips his hand into a small slit under his mattress and pulls out a cell phone. Speed dial connects him to his outside contact, he speaks a few prearranged words, and another drug deal is made. Technology—albeit contraband technology—allows him to operate as if he were still on the streets.

As cell phones become smaller, it becomes easier to smuggle them inside correctional facilities. It becomes easier for inmates to continue their criminal activities, harass victims, or transmit photographs of supposedly secure information.

Fortunately, in today’s technology-driven society, when one innovation creates a problem, a new innovation usually comes along to solve it. But for correctional officers and administrators, the question becomes where to find the right innovation.

“The scope of the problem is this: we are trying to get cell phones out of prisons or at least render them useless,” says Ike Eichenlaub, chief of the Federal Bureau of Prisons’ (BOP’s) Office of Security Technology. To date, several possible technology approaches have been identified to deal with the cell phone problem in prisons and correctional facilities:

(See No More ‘Cell’ Phones, page 12)
As of late fall 2004, more than 50 justice information-sharing projects, including AMBER Alert, iLincs, and ITIP, employ the Global Justice eXtensible Markup Language (XML) Data Model, better known as GJXDM, to facilitate sharing their information with other law enforcement, courts, corrections, and public safety organizations.

GJXDM grew out of a 2001 project to develop common definitions of criminal justice data and promote information sharing among law enforcement, corrections, and public safety organizations. That first effort resulted in the Global Justice XML Data Dictionary, which included more than 300 common justice data elements. Rapid acceptance and implementation of the data dictionary led to the development of a standard framework, or data model, which would fully utilize XML's ability to create information system interoperability.

GJXDM 3.0, released in January 2004, allows disparate computer systems and networks to exchange data more easily by using a common language and set of vocabulary definitions. It is designed to be consistent with major industry and international standards. However, it is flexible enough to be adapted to the needs of specific jurisdictions. The Justice Information Exchange Model (Jiem), developed by SEARCH, the National Consortium for Justice Information and Statistics, is a useful tool for organizations that are planning and implementing projects that use GJXDM. Jiem helps organizations to identify critical information-sharing events. Through its interfaces with GJXDM, Jiem then allows users to incorporate these specified reference exchange points into their database designs.

Ongoing technical development and testing of GJXDM are conducted by the Georgia Tech Research Institute. The Global Justice Infrastructure/Standards Working Group (GJSWG) approves new versions for release; version 3.0.2 was released in September 2004.

The U.S. Department of Justice, Office of Justice Programs won the 2004 American Council for Technology's Interglobal Solutions Award for the GJXDM project. This award goes annually to Federal, State, and local agencies that demonstrate a commitment to progress through collaboration and innovative technology use.

For additional information, visit http://it.ojp.gov.

(About ITIP)

On a September afternoon in 2004, two pre-adolescent girls in North Charleston, South Carolina, reported being followed by a man who had a tattoo on his neck. When a similar report surfaced in Charleston County, the tattoo was identified as that of a lizard. A database search for suspects associated with lizard tattoos in these two locations and surrounding jurisdictions yielded three matches, one of whom was a registered sex offender. The offender, however, provided an ironclad alibi. Police returned to question the girls, who recanted their accusations.

In South Carolina's Low Country the sheriff's departments of Charleston, Berkeley, and Dorchester Counties and the police departments for the municipalities of Charleston, Mount Pleasant, and North Charleston developed a regional information system called the Information Technology Improvement Project (ITIP) to integrate their stand-alone databases and share information electronically across jurisdictional boundaries. “Because of ITIP, our agencies are sharing information, working more cases together, and arresting offenders who are committing crimes in all our jurisdictions,” says Chief Robert E. Groce of the Mount Pleasant Police Department.

ITIP enables line officers to access information about a suspect's involvement in other crimes, not only as a suspect but also as a witness or victim, according to Charleston County Sheriff's Special Enforcement Technology Commercialization, part of the NLECTC–Southeast, located in North Charleston, to help develop a regional information system. NLECTC–Southeast helped develop architectural concepts and operational requirements for the

(See iLincs and ITIP, page 3)
network. The Southeast Center works in partnership with the U.S. Department of Defense, represented by the Space and Naval Warfare Systems Center Charleston; the U.S. Department of Energy, represented by the Oak Ridge National Laboratory and the Savannah River Technology Center; the South Carolina Research Authority (SCRA); and educational institutions, including the Georgia Tech Research Center.

"Integrating justice information is not simply a matter of choosing technology and integrating various computer software or records management systems," notes Coleman Knight, project manager at NLECTC-Southeast. "Agencies that want to integrate and share information need to consider policy decisions such as who is responsible for data, access, and security; legal and liability issues; how the resulting information-sharing system will be governed; and how it will be funded."

Technological and operational issues also must be considered. Agencies must determine what information should be shared, develop operational standards and protocols, choose software and hardware, design security precautions, populate the database, perform acceptance testing, and train users.

Security, Knight says, is critical in designing a shared information system. Law enforcement data is usually highly sensitive. Officers with different duties have access requirements differing levels of confidentiality, and legal requirements for the data. County, state, federal levels vary. "There are real-world political, turf, and trust issues that may affect the development of this kind of project. Agencies may be reluctant to share information gathered from informants and other information sources. There are specific requirements at the State and Federal levels dealing with intelligence information, legal liabilities arising from one agency's misuse of another agency's information, and many other concerns."

According to Knight, the strength of ITIP has been the joint ownership of the executive committee. This ownership is critical, he says, because the executive committee needs the authority as a group to make decisions, manage the system for the benefit of all, and avoid power struggles and potential turf issues. Each agency in an information-sharing system should have an equal voting partner. For ITIP, this means that all agencies have access. Routers are installed at each agency and at SCRA to coordinate information transmission. Firewalls, user codes, and passwords ensure data and user security.

"Of primary concern to the participating agencies was the avoidance of an additional burden on their legacy record management systems, most of which were stretched nearly to the breaking point under normal, everyday operation." Knight says. "So when you run a query, it goes to the central data warehouse instead of going to each agency's database. The ITIP system thus is set up to handle thousands of users simultaneously." ITIP agencies also wanted to segregate their legacy RMS from the shared system to allow each agency to determine which data elements to share. Finally, they wanted to create an environment that would be conducive to exploring data-mining techniques.

Each jurisdiction still maintains and controls its own RMS, which cannot be modified through the ITIP network. A software system replicates data and allows information sharing across jurisdictions regardless of the structure of the underlying data sources. Searches can be done using either a preformatted name query application or an ad hoc query application. The preformatted name query application employs a preset form to search for records based on a name or names and provides results in a preset format; the ad hoc query application allows users to search fields not included in the preformatted form, so users can tailor their queries around such features as age, sex, height, or tattoos.

In automating information sharing, Knight says, "First, do no harm." An automated information-sharing system should lessen the workload and should not negatively affect an RMS or its data. Automating an already bad process will only result in an automated bad process.

Protecting law enforcement agency data is critical because serious legal and liability consequences can arise through mishandling or inadvertently releasing certain categories of information. ITIP's executive committee examined the issues of record expungement, arrest warrants, and juvenile data with special care. Although each agency controls and limits the data that goes into ITIP, each has chosen to share all its data universally. "ITIP has also been a catalyst for more information sharing among law enforcement in general," says North Charleston's Cordray. In addition to the shared database, she says her agency now exchanges e-mails with others regarding significant incidents.

When developing a request for proposal (RFP) to build an ITIP-like system, the more detail, the better. Knight says. If the RFP uses language that is too broad, it is subject to vendor interpretation, which may not be what the agency really wants. Be clear, he says, about what the information-sharing system should do. Provide details about functional requirements. "Requirements can always be removed, but it is hard to add them," he says. Several times in the ITIP implementation process, the working group had to modify or waive requirements.

Some ITIP agencies have changed their RMS over the years. Older data has been moved from one legacy system to another. Older RMS programs tend to have fewer data validation requirements than current ones, resulting in data that is difficult to replicate at best or unusable at worst. Because each agency's hardware and interface was different, a different replication program had to be created to add each agency to the system. In addition, data are not always entered the same way each time, staff originally trained in the system leave, and people understand and perform tasks differently.

"As the system gets up and running, test and retest," Knight says. Quality assurance testing with actual system data will ensure that vendor hardware and software perform to specifications. Failing to conduct quality assurance testing could allow defective hardware or software to be installed, leaving little or no recourse. And finally, says Charleston's Pham, "Contract, contract, contract. Make sure you have a good contract with your vendor. If recurring costs to maintain the system are too high, your agency can't afford it."

For more information about the Low Country Information Technology Improvement Project, contact Coleman Knight, 800-292-4355 or nлектcse@nlectc-se.org.
TechBeat is the award-winning newsmagazine of the National Law Enforcement and Corrections Technology Center (NLECTC) system. Our goal is to keep you up to date with current and developing technologies for the public safety community, as well as other research and development efforts within the Federal Government and private industry. TechBeat is published four times a year.

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

Domestic Department Subscriptions: If your division, department, or agency has more than 20 individuals, we can drop ship as many copies as you require. All you have to do is provide us with the quantity needed, a shipping address (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 20 copies, please provide us with the names and addresses of individuals who are to receive the newsmagazine and we will send copies directly to them. Contact Rick Neimiller, TechBeat managing editor, at 800–248–2742, for additional information or to subscribe.

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

Article Reproduction: Unless otherwise indicated, all articles appearing in TechBeat may be reproduced. We do, however, request that you include a statement of attribution, such as, "This article was reproduced from the Winter 2005 issue of TechBeat, published by the National Law Enforcement and Corrections Technology Center, a program of the National Institute of Justice, 800–248–2742." A bimonthly periodical that highlights recent publication and products and contains a convenient online order form.

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

Ask questions. Share comments. Get answers to your questions or share suggestions about NLECTC services at—

http://askncjrs.ncjrs.org (questions)
http://tellncjrs.ncjrs.org (comments)

NCJRS Contact Information at a Glance

NCJRS Contact Information at a Glance

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

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

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

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

Links
Links takes you to other important law enforcement and corrections websites.

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

6th Annual Innovative Technologies for Community Corrections Conference
June 13–15, 2005
Red Lion Hotel on 5th Avenue • Seattle, Washington

Registration fee: $150 per person (covers the cost of provided meals). The conference will spotlight the innovative use of technology in community corrections and emerging technologies. A vendor exposition will be available for attendees to interact with technology providers.

Tentative topics include—

• Innovative Case Management Systems
• Advances in Electronic Monitoring
• Drug and Alcohol Testing Technologies
• Technology to Manage Sex Offenders
• E-Learning for Community Corrections
• Officer Safety

For more information or to be placed on our mailing list regarding this conference, please call Joe Russo at 800–416–8086, or e-mail jrusso@du.edu.

Hosted by the National Law Enforcement and Corrections Technology Center–Rocky Mountain, a program of the National Institute of Justice.
For already overburdened probation and parole officers, the advent of the personal computer and the Internet has further complicated their caseloads. But a course titled, ‘Managing Sex Offenders’ Computer Use: A 2-Day Technical Training for Probation and Parole Officers’ was offered for training and monitoring of these offenders. The course, began offering the course throughout its 10-State region.

In addition to working with APPA and its consultant, NLECTC–Rocky Mountain also collaborated with individual States, identifying the key community corrections agencies as the training centers. Cases were discussed with those agencies to identify suitable computer labs for the training and appropriate participants to take the course.

“We didn’t want this to be a self-selecting thing,” Russo explains. “We didn’t want someone who is interested, but is not actually supervising sex offenders, to take a look away from someone who really needs it. Rather, participants can take the information and resources back to their workplaces and share the knowledge with their coworkers.”

To run the hands-on course, the instructor needs a 30- to 90-seat computer lab for 2 days, temporarily installing hard drives that contain actual caches of information from sex offenders’ computers. (Although the course includes sexually explicit materials, it does not include child pornography.) Topics covered in “Managing Sex Offenders’ Computer Use” include—

• Understanding sex offenders and the effects of pornography.
• How sex offenders access information.
• Ways in which computers can be involved in crimes.
• Legal issues.
• Technical aspects of computer management.
• Installing appropriate software and selecting text search keywords.
• Examining and cleaning hard drives.

The course teaches probation and parole officers to take a different approach to computer forensics than the one traditionally followed by law enforcement. Russo says, Law enforcement looks at a hard drive as a historical record of evidence used in the prosecution of a crime that has already occurred. Probation and parole officers have a different orientation; they are more concerned with managing and monitoring behavior from this point forward to try to prevent future crime.

“Often during a counseling session,” Russo says, “what a sex offender says is his main sexual interest is not really his main interest. By checking his hard drive, we can find out what he’s really been looking at. This can become a baseline for helping him get the right treatment.” After learning as much as possible about the offender, the officer then wipes the hard drive clean and installs monitoring software so that periodic checks of the hard drive will indicate if the offender has violated his supervision or even committed a new crime.

“Offenders will of course try to beat the software,” he adds. The course instructs officers to equate the computer check to a drug test; offenders may beat a particular test, but anyone who is still a user will eventually get caught. The same principle applies to sex offenders: they might get around monitoring a couple of times, but not forever. The unanimously positive feedback received by the Rocky Mountain Center proves that probation and parole officers need this training to teach them the skills that will ensure violators eventually are caught.

“Officers usually are shocked at the extent of pornography available on the Internet,” Russo says. “The depth and breadth of perversion and the dangers the Internet poses for sex offenders is a slap in the face to them. Officers are used to dealing with offenders’ addictions, joblessness, and family relationships; now they must also deal with online pornography, sex chat rooms and discussion boards, and dating services that target vulnerable, single-mom families with the ‘right type’ of children in the household.”

“After they get over the initial shock,” he says, “then we tell them here are some real tools and a concrete way to manage that risk.”

For more information on ‘Managing Sex Offenders’ Computer Use: A 2-Day Technical Training for Probation and Parole Officers,’ contact Joe Russo at NLECTC–Rocky Mountain, 800–416–8086 or jrusso@du.edu.
I nauguration Day 2005, the first since 9/11, will be filled with concerns for the U.S. Park Police (USPP), which takes the lead in ensuring security and safety for this and other Federal Government events in Washington, D.C. The department will call on dozens of law enforcement, fire, and emergency response agencies from up and down the East Coast for assistance—agencies that use a variety of radio systems, channels, and frequencies.

However, the ability to talk with different public safety agencies with disparate radio systems, termed “interoperability,” should be less of a concern on Inauguration Day because of lessons learned from the ceremonies for the dedication of the World War II Memorial during Memorial Day Weekend 2004.

Memorial Day Weekend 2004 was not just another holiday weekend in the Nation’s Capital. On this Memorial Day, government officials, dignitaries, and tens of thousands of ordinary Americans, many of them World War II veterans, gathered on the National Mall for the dedication of a memorial to those who served and died in World War II.

To ensure that the more than 30 law enforcement agencies and 600 officers involved in the event could communicate, USPP called on Capt. Eddie Reyes of the Alexandria Police Department in nearby northern Virginia. USPP contacted Reyes, who provides technical assistance for the National Institute of Justice’s (NIJ’s) CommTech (formerly AGILE) program, approximately 3 weeks before the dedication. According to Reyes, the timing of this contract led to the most valuable lesson learned:

“The biggest lesson we learned is that for future events on this scale, we need to allocate time. You need at least 2 months to plan something on this scale,” Reyes says. USPP loaded his concerns when planning for Inauguration Day, making initial contact in October 2004.

Even though planning time was somewhat limited, Reyes used his experience establishing interoperability during National Police Week, held in the National Capital Region each May, to pull the Memorial Day operation together. (National Police Week draws between 25,000 and 40,000 attendees each year, according to its official website, with major events taking place across the city and around staying at many hotels.) For help, he called on NIJ’s National Law Enforcement and Corrections Technology Center-Northeast (NLECTC–Northeast) in Rome, New York. Reyes and NLECTC–Northeast staff member Charles Stephenson drafted a letter to all participating agencies asking them about their radio systems and interoperability capabilities. The agencies’ replies were the basis for determining interfaces, an interoperability layout, and needed equipment.

Following the National Police Week model, Reyes and Stephenson incorporated three interoperability strategies into the World War II Memorial dedication plan to enable emergency communications:

1. Distribute loaner radios from National Capital Region law enforcement agencies. An officer using a loaner radio can communicate with all other officers who have similar radios, as well as the command post and others using the same channel. During the World War II Memorial dedication weekend, platoon leaders from each participating agency received radios that were tuned to a common channel and connected through a modular interface/interconnect system. This interface added monitoring capability and could provide a patch between four additional radio systems if needed.
2. Capitalize on existing interoperability systems. Many law enforcement agencies in the National Capital Region use 800 MHz radios, which can be programmed for compatibility with other agencies’ 800 MHz systems.
3. Establish interconnect switches. Not all agencies use 800 MHz radios, many use UHF or VHF devices. Connecting those systems requires an intermediary switch like an ACU–1000 or similar system. Such a switch provides direct connectivity between radio systems that operate at different frequency bands such as VHF, UHF, and 800 MHz. Reyes and the USPP planning team called on the expertise of NLECTC–Northeast and NIJ personnel to help establish this connection.

On the Friday before Memorial Day, staff from NLECTC–Northeast, NIJ, and the Alexandria Police Department barricaded an entire block near the Franklin Delano Roosevelt Memorial to set up a communications command post. The team erected a 108-foot antenna mast loaned by the U.S. Marshals Service, deployed an 800 MHz portable repeater belonging to the Fairfax County (Virginia) Police Department, and tested the setup. (The repeater used a national interoperability channel, and all agencies using 800 MHz radios were instructed to preprogram them to the same channel. The ACU–1000 the repeater needed to be moved from its initial position, a low area near the water, to higher ground.

Early Saturday morning, team members met to make sure that all capabilities remained operational. Participating officers received their deployment assignments, and emergency medical services and fire department vehicles and command posts were stationed in the same block.

Stephenson trained the interconnect operator and was on call for technical assistance throughout the event. He said that what made the operation successful was “everything working as expected.”

The event went “really well” despite a glitch that, according to Reyes, led to a valuable lesson learned: “We never did a roll call. We told agencies what channel to use, but we never checked to see if they were using it. We will do a roll call for the inauguration.” Reyes noted that one agency reported a case of heat exhaustion. “We were able to send emergency response out right away. So, as long as the agencies did tune in, they did indeed have interoperability capability.”

Another lesson learned, Reyes says, involved distribution of the loaner radios. For Inauguration Day, the coordinating team is implementing a barcode/scanner checkout system that eliminates the paperwork formerly needed to check out each radio. During the World War II Memorial dedication, some radios were inadvertently checked out without paperwork, but all were returned.

“Anything that initially seems to be a problem, we can turn into a positive by saying, ‘This is how we will do it better next time.’” Reyes adds.

Developing and deploying a mobile communications infrastructure like that required for the World War II Memorial dedication requires extensive teamwork. SCI Industries (a provider of interoperable antenna systems), the Arlington County (Virginia) Police Department, the Metropolitan Washington Airports Authority Police Department, and the U.S. Department of Homeland Security, Immigration and Customs Enforcement played key collaborative roles. The Capital Wireless Integrated Network was used to log incidents called in by officers throughout the day and provide dedicated channels for police, fire, and rescue personnel.

For more information regarding the interoperability initiative for the dedication of the World War II Memorial, contact Capt. Eddie Reyes, 703-638-6060, ext. 184, or Charles Stephenson, NLECTC–Northeast, 315-339-6184.

What is CommTech?

Because communication can mean the difference between life and death, public safety agencies from different disciplines and different jurisdictions need to share information seamlessly—when and where it is needed. Unfortunately, police officers, firefighters, emergency medical personnel, and other public safety officials and responders often cannot depend on wireless radio communications in an emergency. This lack of interoperability hinders a coordinated response to natural disasters, catastrophic accidents, or crimes. It means police, firefighters, and emergency response personnel cannot always talk. And if they cannot talk, they cannot respond.

Interoperability is one of the research missions of the National Institute of Justice (NIJ) and its CommTech (formerly AGILE) program. CommTech is identifying, adopting, and developing interoperability solutions that include open architecture standards for voice, data, image, and video communication systems. These solutions will allow multiple parties to exchange information on the spot—no matter where that “spot” is. They will let users exchange information among fixed, mobile, and personal devices. In addition, CommTech looks for new technology solutions when existing technologies fall short. It also aims to raise awareness of interoperability issues through outreach programs so policymakers and public safety leaders can make informed and cost-effective decisions.

For more information about CommTech, visit www.agileprogram.org.
On just such a morning in 1995, members of the Aum Shinrikyo cult struck against the passengers on the Tokyo subway system. At a predetermined time, cult members used umbrel­la tips to puncture newspaper-wrapped bags of the liquid nerve agent sarin as they got off their trains. By the time it was all over, 12 people had died and thousands who touched the liquid itself or inhaled its vapors were injured.

Through the efforts of the National Institute of Justice (NIJ), the Technical Support Working Group (TSWG), and TIAX LLC, a collaborative research and development company, the likelihood of a similar attack in the United States should be reduced dramatically in the near future. A prototype personal monitor, small enough to wear on a belt and affordable (about $100 per unit), may be available before the end of 2005. The device will warn law enforcement officers and other first responders of the presence of nerve agents well before their effects can be felt.

Nerve agents, when inhaled, ingested, or brought into contact with the skin or the eyes, interfere with the central nervous system, says David Clopton, a contractor with the National Institute of Justice. They disrupt bodily functions by attacking a class of enzymes called cholinesterases. When there is too little of the enzyme acetylcholinesterase (AChE), known as the body’s “off switch,” the neurotransmitter acetylcholine builds up and over­whelms receptors with constant stimulation. The muscles quit work­ing and, ultimately, a person stops breathing.

The personal alarm monitor is essentially “a raw nerve ending in a box,” Clopton says. The nerve agent detection device constantly measures the activity of an AChE sample immobilized in porous plastic. When the enzyme is active, the reagent turns bright yellow; if it is exposed to a nerve agent, the reagent becomes clear and an alarm sounds. When the wearer hears the alarm, he or she can also check a visual indicator to confirm the presence of a nerve agent. The AChE enzyme used is specific to nerve-type toxins, drastically reducing the possibility of false alarms. Also, the alarm is set at the level of the initial physiological response, not at a lethal level, giving the first responder time to assess and react to the situation.

Laboratories already use similar reagents to test blood samples for possible exposure. TIAX, however, came up with a way to continuously monitor the air for exposure in the field by developing a consumable packet that lasts 12 hours and can easily be replaced at the start of a shift. TIAX tested its innovation against simulated nerve agents and arranged for tests against real sarin and soman at the U.S. Army’s Edgewood Chemical and Biological Center. An early prototype of the monitor was also evaluated by several public safety agencies under operational conditions. These included the Washington (D.C.) Area Metropolitan Transit Authority Police, New York City Fire Department, and Los Angeles County Terrorism Early Warning Group. TIAX modified its prototype based on the results of the evaluations. Because Congress transferred the funding and mission for the development of chemical, biological, radiological, and nuclear protective equipment to the Department of Homeland Security, NIJ has forwarded the personal alarm monitor project to the Science and Technolo­gy Directorate of DHS for completion.

Because TIAX was all over, 12 people had died and thousands who touched the liquid itself or inhaled its vapors were injured. For more information regarding the personal alarm monitor project, contact Chris Tillery, 202–305–9829 or george.tillery@usdoj.gov. Editor’s Note: The Technical Support Working Group (TSWG) is a national forum that identifies, prioritizes, and coordinates interagency and international research and develop­ment requirements for combating terrorism. For more information about TSWG, visit www.tswg.gov.

For indepth information and additional resources regarding the nerve agents listed above, visit the following pages on the Internet site for the Centers for Disease Control and Prevention.

Tabun (GA) | Sarin (GB) | Soman (GD) | VX
--- | --- | --- | ---
**Physical Properties**
Organophosphate compounds.
Colorless as liquid or vapor.
Have no odor or have a fruity order.
May be aerosolized.
Decompose with water.
Addition of catalyst (bleach) accelerates decomposition.
**Symptoms**
Salivation.
Constricted pupils.
Watery eyes and runny nose.
Difficulty breathing.
Vomiting.
Convulsions.
Paralysis.
Respiratory failure.
Death.
**Characteristics**
Attack skeletal muscle receptors.
Attack smooth muscle and central nervous system.
Individual susceptibility will differ.
G agents (tabun, sarin, and soman) semipersistent (minutes to hours).
V agent (VX) persistent (days to weeks).
**Routes of Exposure**
Inhalation.
Dermal (eyes and skin).
Ingestion.
**Treatment**
Antidotes include atropine, pralidoxime chloride, and diazepam.
Decontaminate skin by washing with large amounts of soap and water.
Secondary exposure can occur from contact with contaminated clothing. (It can also occur when tabun evaporates from contaminated clothing.)
To protect health care workers and others exposed to a contaminated victim, remove, bag, and seal the victim’s clothing and wash the victim’s skin with large amounts of soap and water.

For more information regarding the nerve agents listed above, visit www.bt.cdc.gov/agent/soman/basics/facts.asp
VX: www.bt.cdc.gov/agent/vx/basics/facts.asp

Note: Information applies to all nerve agents unless a particular agent is named.

For metropolitan transit systems across the Nation, it’s a typical morning. But this morning could turn out not to be typical. This could be the morning terrorists plan to strike with a nerve agent.

...
Better Bomb: To Build or Not to Build

Explosives 101

Although bomb remediation and disposal personnel possess a depth of expertise in explosives and evidence collection, the average first responder—whether police officer, firefighter, or paramedic—often lacks the basics. During the past year, the National Institute of Justice’s National Law Enforcement and Corrections Technology Center (NLECTC)—Rocky Mountain has been working with the local chapter of the International Association of Bomb Technicians and Investigators to educate Colorado’s first responders about bombs and explosives through its Basic Explosives/Evidence Course for First Responders.

“The objective of this course is to show that crime scene investigators can make or break the case,” says Paul Reining, program manager for explosive devices at NLECTC—Rocky Mountain. “We show the participants examples of military-type explosives that find their way to the street, stolen commercial explosives, and homemade devices such as the ones built by the students involved in the incident at Colorado’s Columbine High School in April 1999.”

Basic familiarity with bombs and explosives is not the only goal of the 3-day course, which was offered four times during 2004. “We look at the effects of airblast from an explosion, which can collapse the lungs or damage other organs,” Reining says. “We examine both Federal and State laws pertaining to the ownership, storage, and transportation of explosives. We also point out that State laws can be more restrictive than Federal laws.”

On the final day of the course, Reining says, participants travel to NLECTC—Rocky Mountain’s Explosives Facility to see the effects of a small pipe bomb. Participants join in evidence collection when a car containing a briefcase with two sticks of dynamite, a clock, and a cell phone is blown up. “What surprises them,” Reining says, “is just how far the evidence is dispersed. We end up using a truck load of yellow crime scene tape.”

Although the Rocky Mountain Center administers the course, the instructors—all volunteers—come from public safety agencies in Colorado, including the Denver Police Department, Arapahoe County Sheriff’s Office, Colorado Springs Police Department, Jefferson County Sheriff’s Office, and Denver Health Paramedic Division, among others. “Even the cars that were blown up were donated,” Reining adds.

For more information about the Basic Explosives/Evidence Course for First Responders and other explosive detection and neutralization initiatives of NLECTC—Rocky Mountain, contact Paul Reining, 800–416–8086 or preining@du.edu.

In the late 1990s, the National Institute of Justice (NIJ) funded the development of an affordable, portable containment vessel designed for pipe bombs because they are the most prevalent type of explosive devices faced by bomb squads. The prototype containment vessel, however, failed when it was tested by the National Law Enforcement and Corrections Technology Center (NLECTC)—Rocky Mountain in Denver, Colorado, which serves as NJ’s “Bomb Center,” assisting in the identification of bomb squad technology requirements and supporting the National Bomb Squad Commanders’ Advisory Board (NBSAB).

According to NIJ Deputy Assistant Director Chris Tillery, before NIJ would commit to additional resources and funding to rectify the problem with the prototype, the agency asked the Rocky Mountain Center to determine how high a priority having such a containment vessel was to bomb squads and what that vessel should be designed to do. In response, NLECTC—Rocky Mountain conducted a needs assessment survey that included seven ranked questions (“not important” through “very important”) and three open-ended questions. The survey was administered to 61 certified bomb technicians. The results showed that only a slight majority (56 percent) felt that a lightweight portable bomb containment vessel would be a priority for State and local bomb squads, you would be wrong.

“I hear you think about it, this make a lot of sense,” he adds. “Neutralizing a device in situ reduces the risk to bomb technicians because they don’t have to handle it. Moving explosive devices risks setting them off. Putting an explosive device in a ‘blast proof’ trash container or covering it with a bomb blanket or other similar means of mitigation only complicates the bomb technicians’ job.”

Tillery notes that although NIJ is currently not investing additional funding for the development of bomb containment vessels, it is actively developing other tools to address bomb squad technology requirements. To define requirements, NIJ is working with NBSAB, through NLECTC—Rocky Mountain. In addition, NIJ is working with various technology partners, including the FBI, the Bureau of Alcohol, Tobacco, Firearms and Explosives, various U.S. Department of Defense agencies, the Technology Support Working Group, and the U.S. Department of Homeland Security.

NIJ’s efforts are focusing on information technology, radio-controlled bomb mitigation, and suicide bomber detection. These efforts have produced an affordable bomb robot that meets more than 90 percent of the performance requirements called for by bomb squads (see “Building a Better Bomb Robot,” TechBeat, Summer 2004). Also, an NIJ-funded effort to establish a national strategy to deal with radio-controlled bombs was put in place at the end of 2004. Also in 2004, the agency began a prototype for a real-time, collaborative information-sharing system that would enable a bomb technician anywhere in the United States to obtain access to bomb data and to share that information with any other bomb technician.

For more information about the NIJ Explosive Detection and Remediation Program, contact Chris Tillery, 202–305–9829 or george.tillery@usdoj.gov.
The National Law Enforcement and Corrections Technology Commercialization (NLECTC) system, a program of the National Institute of Justice (NIJ), offers no-cost assistance in helping agencies large and small implement current and emerging technologies.

Technology Commercialization
The NLECTC system was established in 1994 by NIJ’s Office of Science and Technology to deliver information and technology assistance to more than 18,000 police departments; 50 State correctional systems; thousands of prisons, jails, and parole and probation departments; and other public safety organizations.

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

Technology Demonstration
We introduce and demonstrate new and emerging technologies through such special events, conferences, and practical demonstrations as the Mock Prison Riot (technologies for corrections) 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
We provide hands-on demonstrations of the latest technologies to address such operational issues as crime and intelligence analysis, geographic information systems, explosives detection and disassembly, and technology availability, performance, durability, reliability, safety, ease of use, customization capabilities, and interoperability.

Technology Information Network (JUSTNET)
The NLECTC system provides information to the criminal justice community at no cost through educational bulletins, equipment performance reports, guides, consumer product lists, news summaries, meeting conference reports, videotapes, and CD-ROMs. NLECTC also publishes TechBeat, an award-winning quarterly newsmagazine. Most publications are available in electronic form through the Justice Technology Information Network (JUSTNET) at www.justnet.org. Hard copies of all publications can be ordered by calling 800–248–2742, or via e-mail at asknlectc@nlectc.org.

Technology Commercialization
Our law enforcement and corrections professionals, product and commercialization managers, engineers, and technical and market research specialists work together to identify new technologies and product concepts. They then work with innovators and industry to develop, manufacture, and distribute these new, innovative products and technologies.

Technology Needs Assessment
Our national body of criminal justice professionals—the Law Enforcement and Corrections Technology Advisory Council (LECTAC)—ensures that we are focusing on the real-world needs of public safety agencies.

Because most of the 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. Most centers and offices are collocated with or supported by federally funded technology partners so they can leverage unique science and engineering expertise.

Contact NLECTC for:
A Review: Technologies in Development

NLECTC–Southeast

Well over a dozen National Institute of Justice-funded technologies in development were reviewed and discussed during the Institute’s annual Technology Grant In-Process Review held in conjunction with the International Association of Chiefs of Police (IACP) Law Enforcement Information Management Conference last spring in Sacramento, California. NLECTC–Southeast hosted the discussion of lessons learned on technology projects that included the—

• Automated Regional Justice Information System, a complex criminal justice network used by 51 local, state, and federal agencies in San Diego and Imperial Counties, California.

• Capital Wireless Integrated Network, a wireless system of integrated transportation and criminal justice information in Maryland, Virginia, and the District of Columbia.

• Voice over Internet Protocol, one of the leading technologies for the digital encoding and transportation of voice over IP networks.

• Software System for Information Extraction project, designed to take advantage of the tremendous amount of law enforcement information available in narrative reports to solve crimes.

• National Software Reference Library, a physical collection of software that contains more than 5,300 software packages and a software database of file “fingerprints” and additional information that uniquely identifies each of 18 million files.

Go to www.justnet.org/nlectcse/download/LEIMreview04.pdf for a downloadable report about these and other reviewed technologies. For more information about the IACP’s Law Enforcement Information Management Conference, visit www.iacptech.org/2004LEIM.htm.

Responding to a Changing Technological Environment

NLECTC–National

The Law Enforcement and Corrections Technology Advisory Council (LECTAC) is the primary “big picture” link between the law enforcement and corrections community and the science and technology programs of the National Institute of Justice (NIJ). LECTAC members include representatives from Federal, State, local, and international criminal justice agencies and organizations. Since its inception, LECTAC has been reorganized as needed. In a post 9/11 world, LECTAC continues to be responsive to a rapidly changing technological environment, providing a better understanding of real-time operational requirements of the public safety community. To that end, LECTAC will soon team up with technical working groups to provide NIJ and the NLECTC system with an accurate, realistic set of operational requirements and technology. The working groups will be sponsored and guided by the various centers and offices of the NLECTC system and will be composed of persons within the public safety community, scientific/ research community, and industry. By working together, LECTAC and the working groups can examine criminal justice technology needs from many different aspects, from the perspective of the first responder to that of policymakers and administrators. LECTAC is administered by NLECTC–National. For more information, contact Barry Bratbud, 800–248–2742 or bratbud@nlectc.org.

Database of Weapons in Disguise

Office of Law Enforcement Technology Commercialization (OLETC)

A knife concealed inside a key… a ring that fires a single 22-caliber bullet… a hollowed-out soda machine to hide firearms… a pistol hidden in a cam-corder. OLECt’s Disguised Weapons Project is a database containing information and photos of disguised, concealed, and unusual weapons.

Since the project’s inception in 2001, the database has grown continuously and now includes almost 400 disguised and concealed weapons. The database has been incorporated into a PowerPoint® presentation that can be accessed by public safety personnel via the Internet. The information is protected by an online registration system through which employment with a bona fide public safety agency is verified before a password is issued. For more information about the Disguised Weapons Project or to request a password, contact Bill Patsche, 888–306–5382 or wpatsche@oletlec.org.

Spatial Forecasting in Tactical Crime Analysis

NLECTC–Rocky Mountain

During the summer of 2004, NLECTC–Rocky Mountain completed a survey of crime analysts on the use of spatial forecasting techniques in tactical crime analysis. Spatial forecasting involves the use of statistical techniques to predict the area of a future event in a crime series. Survey results show a strong interest in spatial forecasting, but analysts are unfamiliar with the wealth of tools within a geographic information system (GIS) to accurately predict the “hunting grounds” of the offenders who are committing these crimes. A project to determine the most accurate of the various GIS techniques available is underway. Solving crime series from across the Nation are being tested for success using the various spatial techniques. Goals of the project include educating the crime analysis community, developing a methodology to approach spatial forecasting as a crime analyst, finding the most accurate technique available, and providing a base for future research in spatial forecasting. For more information, contact John Van Aaken, 303–871–3946 or jvanauke@du.edu.

Digital Imaging for Safer Schools

National Institute of Justice

The counties of Arlington and Fairfax in Virginia are no strangers to adversity. Arlington is home to over 23 days in October 2002 trying to catch a serial sniper, who was caught and is verified before a password is issued. The project, designed to take advantage of the digital encoding and transportation of voice over IP networks.

software system of integrated transportation and criminal justice information in Maryland, Virginia, and the District of Columbia. NLECTC–Southeast hosted the discussion of lessons learned on technology projects that included the—

• Automated Regional Justice Information System, a complex criminal justice network used by 51 local, state, and federal agencies in San Diego and Imperial Counties, California.

• Capital Wireless Integrated Network, a wireless system of integrated transportation and criminal justice information in Maryland, Virginia, and the District of Columbia.

• Voice over Internet Protocol, one of the leading technologies for the digital encoding and transportation of voice over IP networks.

• Software System for Information Extraction project, designed to take advantage of the tremendous amount of law enforcement information available in narrative reports to solve crimes.

• National Software Reference Library, a physical collection of software that contains more than 5,300 software packages and a software database of file “fingerprints” and additional information that uniquely identifies each of 18 million files.

Go to www.justnet.org/nlectcse/download/LEIMreview04.pdf for a downloadable report about these and other reviewed technologies. For more information about the IACP’s Law Enforcement Information Management Conference, visit www.iacptech.org/2004LEIM.htm.

Responding to a Changing Technological Environment

NLECTC–National

The Law Enforcement and Corrections Technology Advisory Council (LECTAC) is the primary “big picture” link between the law enforcement and corrections community and the science and technology programs of the National Institute of Justice (NIJ). LECTAC members include representatives from Federal, State, local, and international criminal justice agencies and organizations. Since its inception, LECTAC has been reorganized as needed. In a post 9/11 world, LECTAC continues to be responsive to a rapidly changing technological environment, providing a better understanding of real-time operational requirements of the public safety community. To that end, LECTAC will soon team up with technical working groups to provide NIJ and the NLECTC system with an accurate, realistic set of operational requirements and technology. The working groups will be sponsored and guided by the various centers and offices of the NLECTC system and will be composed of persons within the public safety community, scientific/ research community, and industry. By working together, LECTAC and the working groups can examine criminal justice technology needs from many different aspects, from the perspective of the first responder to that of policymakers and administrators. LECTAC is administered by NLECTC–National. For more information, contact Barry Bratbud, 800–248–2742 or bratbud@nlectc.org.

Database of Weapons in Disguise

Office of Law Enforcement Technology Commercialization (OLETC)

A knife concealed inside a key… a ring that fires a single 22-caliber bullet… a hollowed-out soda machine to hide firearms… a pistol hidden in a cam-corder. OLECt’s Disguised Weapons Project is a database containing information and photos of disguised, concealed, and unusual weapons.

Since the project’s inception in 2001, the database has grown continuously and now includes almost 400 disguised and concealed weapons. The database has been incorporated into a PowerPoint® presentation that can be accessed by public safety personnel via the Internet. The information is protected by an online registration system through which employment with a bona fide public safety agency is verified before a password is issued. For more information about the Disguised Weapons Project or to request a password, contact Bill Patsche, 888–306–5382 or wpatsche@oletlec.org.

Spatial Forecasting in Tactical Crime Analysis

NLECTC–Rocky Mountain

During the summer of 2004, NLECTC–Rocky Mountain completed a survey of crime analysts on the use of spatial forecasting techniques in tactical crime analysis. Spatial forecasting involves the use of statistical techniques to predict the area of a future event in a crime series. Survey results show a strong interest in spatial forecasting, but analysts are unfamiliar with the wealth of tools within a geographic information system (GIS) to accurately predict the “hunting grounds” of the offenders who are committing these crimes. A project to determine the most accurate of the various GIS techniques available is underway. Solving crime series from across the Nation are being tested for success using the various spatial techniques. Goals of the project include educating the crime analysis community, developing a methodology to approach spatial forecasting as a crime analyst, finding the most accurate technique available, and providing a base for future research in spatial forecasting. For more information, contact John Van Aaken, 303–871–3946 or jvanauke@du.edu.

Digital Imaging for Safer Schools

National Institute of Justice

The counties of Arlington and Fairfax in Virginia are no strangers to adversity. Arlington is home to over 23 days in October 2002 trying to catch a serial sniper, who was caught and is verified before a password is issued. The project, designed to take advantage of the digital encoding and transportation of voice over IP networks.

software system of integrated transportation and criminal justice information in Maryland, Virginia, and the District of Columbia. NLECTC–Southeast hosted the discussion of lessons learned on technology projects that included the—

• Automated Regional Justice Information System, a complex criminal justice network used by 51 local, state, and federal agencies in San Diego and Imperial Counties, California.

• Capital Wireless Integrated Network, a wireless system of integrated transportation and criminal justice information in Maryland, Virginia, and the District of Columbia.

• Voice over Internet Protocol, one of the leading technologies for the digital encoding and transportation of voice over IP networks.

• Software System for Information Extraction project, designed to take advantage of the tremendous amount of law enforcement information available in narrative reports to solve crimes.

• National Software Reference Library, a physical collection of software that contains more than 5,300 software packages and a software database of file “fingerprints” and additional information that uniquely identifies each of 18 million files.

Go to www.justnet.org/nlectcse/download/LEIMreview04.pdf for a downloadable report about these and other reviewed technologies. For more information about the IACP’s Law Enforcement Information Management Conference, visit www.iacptech.org/2004LEIM.htm.
Locate cell phones and confiscate them. This approach, Eichenlaub says, requires a technology that, at a minimum, will—

- Work even when cell phones are turned on for only a few minutes at a time.
- Detect signals emanating from any area of a facility.
- Find transmissions through thick concrete walls, in buildings that range from single story to multi-floored, and in locations varying from urban downtown areas to remote rural districts.

Ideally, he says, such a technology would require minimal or no training to use; expand to cover other wireless technologies, such as two-way pagers; and operate on a 24/7 basis.

**Overpower the signal with a stronger signal.** "Another potential approach is commonly referred to as ‘jamming,’ which emits a signal stronger than a cell phone’s signal and renders it useless," Eichenlaub says. Senior BOP Technologist Jim Mahan adds, "There are two types. One is called brute force jamming, which just blocks everything. The problem is, it’s like power-washing the airwaves and it bleeds over into the public broadcast area. The other puts out a small amount of interference, and you could potentially confine it within a single cell block. You could use lots of little pockets of small jamming to keep a facility under control."

"Trick" the phone. Eichenlaub describes a third possible approach, commonly called "spoofing," as tricking the cell phone into thinking a "no service" signal is coming from the nearest cell tower.

The Federal Communications Commission, however, prohibits both jamming and spoofing, he says, so implementing either of these technologies would require legal and regulatory changes.

**Intercept the signal.** A fourth possible approach, signal interception, retrieves the telephone and serial numbers from operational phones, but it can be implemented only under a judge’s order.

Eichenlaub says that although signal interception is feasible, "We are looking for the simplest option, which is signal detection. There are no regulatory or legal issues here; if you can find it, you can go get it."

Different cellular providers use different communications protocols, but all cell phones use radio frequency (RF) antenna power. BOP has studied a number of off-the-shelf technologies to detect RF signals. Although a variety of detection equipment is available, costs can reach tens of thousands of dollars. "Some [technologies] work better than others," Mahan adds. "Some work for only a short distance, maybe about 15 to 20 feet. This is impractical if you’re trying to cover 50 acres. Also, each device may cost about $1,000. There is some promising new technology that is showing better results than anything else we’ve ever seen, but they are still prototypes. The question is whether the technology can be made at a cost that we can afford. Vendors would need to reengineer solutions originally developed for other professions, such as the military, first responders, or law enforcement."

"I think that a solution can be developed, but there are none out there that meet BOP’s needs right now," Eichenlaub adds.

In response, BOP, the National Institute of Justice (NIJ), and the Naval Surface Warfare Center–Dahlgren are collaborating on a multiyear project to evaluate the problem and ultimately help that technology develop. BOP spent the first 6 months of 2004 evaluating and testing various possibilities. Now Dahlgren staff members (with NIJ funding) are going to evaluate the entirety of the problem and potential technical solutions to provide a roadmap to addressing this problem. In the course of this evaluation, they will—

- Analyze and document BOP’s work.
- Discuss this issue with the American Correctional Association and the Association of State Correctional Administrators to ascertain the needs of State and local correctional institutions and determine how they might differ from BOP requirements.
- Assess the spectrum of potential approaches and technology solutions.
- Ultimately, incorporate BOP’s work and other information into a report that recommends NIJ’s next technology development steps.

Chris Tillery, project manager for NIJ, says he expects that report to be completed and released later in FY 2005.

For more information on the Federal Bureau of Prisons’ research into cell phone use by inmates, contact Ike Eichenlaub, 202–305–8448 or IEichenlaub@bop.gov. For more information on the National Institute of Justice’s involvement, contact Chris Tillery, 202–305–9829 or george.tillery@usdoj.gov.

---

*No More 'Cell' Phones... cont. from page 1*