It’s evident that the Nation’s small and rural law enforcement agencies have a need for low-cost alternatives to planes and helicopters that would allow them to perform aerial surveillance for missing children, lost hikers, and illicit marijuana fields, just like many of their larger counterparts. In response, the Office of Justice Programs’ National Institute of Justice (NIJ) has been looking at a number of options and since September 2005 has been conducting field demonstrations with a pair of powered parachutes. NIJ is now ready to expand those demonstrations to include law enforcement agencies.

According to Mike O’Shea, NIJ program manager, powered parachutes are two-seater ultralight craft that fly with a parachute as their wing. Should the engine fail, the craft simply drifts, under the parachute, to the earth. These ultralight craft have a range of about 100 miles and a top speed of about 30 miles per hour. Powered parachutes fly on mid-grade (89 octane) gasoline that can be purchased at any service station, although they can also use the more expensive 100-octane low-lead aircraft fuel commonly found at most airports.

As for flying powered parachutes, O’Shea says they are relatively easy to learn to fly. “The steering is very simple,” he says. “You push the steering bar with your foot to the left to go left, to the right to go right, and you add throttle to go up and less to go down. They have dual controls so they can be flown from either seat.”

O’Shea points out that the aircraft can become difficult to launch in winds greater than 15 miles an hour, and although they can be flown in cold weather, pilots/passengers are exposed to the elements and it can be quite cold. However, it is not uncommon for pilots to bundle up and fly in subfreezing temperatures. Stiffer winds can sometimes force a craft to land a short distance from where it took off; it took only one such experience for O’Shea to understand why his instructor told him to sit on the empty parachute bag and take it along for the ride. “I had to tuck the chute under the craft to keep it from blowing, walk back to the takeoff point for the bag, and carry the bag back to pack up the chute,” he says. “If I had had it with me, I could have packed the chute on the spot and just driven it back across the grass to the storage area.”

On the positive side, O’Shea says powered parachutes have the advantage of being able to take off out of any unimproved field, which would be a distinct advantage in small and rural counties that lack airports.

Also a positive is the cost of a powered parachute. “The cost, around $15,000, is extremely attractive,” O’Shea says. “Many law enforcement agencies—even the larger ones—just can’t afford an aircraft, either helicopter or fixed wing. Small and rural agencies used to be able to call on larger agencies and National Guard aircraft, but because of rising fuel prices and military deployments, these aircraft are only available in the direst of circumstances.

“Ideally, the craft could be used by coalitions of two or three agencies, because not every small and rural agency would need a craft full time; this would further reduce the costs and increase the use of the aircraft.”

O’Shea adds that during NIJ’s initial field demonstrations (See Under Your Own Power, page 10)
Online News Summary. Online News Summary includes article abstracts on law enforcement, corrections, and forensics technologies that have appeared in major newspapers, magazines, and periodicals and on national and international wire services and websites.

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

Publications. Publications from NIJ and NLECTC that you can view or download to your system, including printer-friendly versions of TechBeat articles and features.

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.

We Did It Again!

TechBeat is the award winning newsmagazine of the National Law Enforcement and Corrections Technology Center (NLECTC) system. TechBeat’s latest award is the APEX 2006 Award of Excellence–Newsletters–Print. 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 Spring 2006 issue of TechBeat, published by the National Law Enforcement and Corrections Technology Center, a program of the National Institute of Justice, 800–248–2742.”

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

Photo Credits: Photos used in this issue of TechBeat copyright © 2006 Alamy; Getty Images; Veer; Photodisc; U.S. Postal Inspection Service; Brian Lewis; and College of Justice Safety, Eastern Kentucky University.

Staff: Managing Editor, Rick Neimiller; Editor, Michele Coppola; Assistant Editor, Janet McNaughton; Lead Writer, Becky Lewis; Contributing Writers, Vaughn Deckret and Lori Abrams; Graphic Designers, Cheryl Denise Collins and Tina Kramer.

CRIME MAPPING RESEARCH CONFERENCE

March 28–31, 2007

Omni William Penn Hotel • Pittsburgh, Pennsylvania

9th CRIME MAPPING RESEARCH CONFERENCE

March 28–31, 2007

Focus:
• Spatial Approaches to Understand Crime and Demographics
• Developing Methods for Research and Practice

Issues to be Discussed Include:
• Use and development of methodologies for practitioners and researchers
• Technical solutions

As a law enforcement arm of the Postal Service, it’s our responsibility to respond to threats in the mail, and we recognized the need to enhance our capabilities,” Brinkley says. “Postal inspectors have investigated threatening mail and suspected explosive devices for more than a hundred years, and we had the equipment for those threats, but bioterrorism added a new dimension. We quickly realized that we needed additional tools to ensure employees and the public were safeguarded while minimizing the effect on postal operations.”

A biohazard detection system for mail processing equipment was developed for the Postal Service after the anthrax attacks. The system sounds an alarm if anthrax is detected. In addition, to ensure a rapid, mobile response to unidentified substances found in the mail and easy access to field screening equipment, the Inspection Service ordered 35 specially equipped SUV response vehicles. The vehicles, which are deployed strategically for use in all 50 States and Puerto Rico, are used to transport field screening and response equipment to reports of suspicious substances in the mail, possible explosive devices, or any biohazard detection system alert.

“We’ve had a lot of interest from other law enforcement agencies that want a similar type of vehicle,” Brinkley adds. “The feedback on the trucks has been excellent. Everything our inspectors need is in one place, the vehicle will get there in any kind of weather, and it brings all the tools they need to assess a suspicious item at the scene.”

Brinkley says a company that specializes in response vehicles and ambulances provided the SUVs—four-wheel-drive Chevrolet Suburbans with large gasoline engines, a towing package, and heavy-duty suspension. They have storage and work areas, the ability to run alternating current (AC) and direct current (DC) from the back of the vehicle, and other modifications that provide a mobile platform to support inspectors’ assessments of unidentified substances and suspicious mail. They also have additional lighting, security, and the latest UHF and VHF encryption-ready radios to enable inspectors to communicate with other public safety agencies.

Specific features include the following:
- Customized rear storage area configured for portable x-ray equipment, evidence collection supplies, and other gear and equipment, with multiple locking compartments.
- Pull-out work shelf.
- Built-in 3,000-watt power inverter (coupled with a high-output alternator and twin battery system).
- 110-volt AC and 12-volt DC outlets in the front and rear to power all equipment.
- Magnet-mounted floodlights for scene lighting (extension cords allow them to be moved to distant scenes).
- Siren; public address system; and covert front, rear, and side emergency lights.
- Engine idler and override (the ignition key can be removed with the engine running at increased idle, providing electrical power while the vehicle is secured).
- UHF and VHF radios for multiple communication capabilities. Each radio holds 250 programmed frequencies, with encryption if necessary, allowing postal inspectors to communicate with any other law enforcement agency or first responders in the area.

---

**Types of Anthrax**

**Skin (cutaneous).** The first symptom is a small sore that develops into a blister, then into a skin ulcer with a black area in the center. In most cases, early treatment with antibiotics can cure cutaneous anthrax. Even if untreated, 80 percent of people who become infected with cutaneous anthrax survive.

**Lungs (inhalation).** Initial symptoms may resemble a common cold—sore throat, mild fever, muscle aches, and malaise. After several days, the symptoms may progress to severe breathing problems and shock. Inhalation anthrax is usually fatal.

**Digestive (gastrointestinal).** Initial signs of nausea, loss of appetite, vomiting, and fever are followed by abdominal pain, vomiting of blood, and severe diarrhea. Intestinal anthrax results in death in 25 percent to 60 percent of cases.

**Treatment**

Antibiotics are used to treat all three types of anthrax. Early detection and treatment are important.

**Prevention after exposure.** Treatment is different for a person who has been exposed to anthrax but is not yet sick. Health care providers will use antibiotics combined with the anthrax vaccine to prevent anthrax infection.

**Treatment after infection.** Treatment is usually a 60-day course of antibiotics. Success depends on the type of anthrax and how soon treatment begins.

**Information Source:** Centers for Disease Control and Prevention website, [www.bt.cdc.gov/agent/anthrax/needtoknow.asp](http://www.bt.cdc.gov/agent/anthrax/needtoknow.asp)
That effectiveness came to bear for George J. Stallworth, a probation and parole officer for the Sex Offender Unit of Tennessee’s Board of Probation and Parole, and Dan Newby, a parole and probation officer and fugitive investigator for Iowa’s 4th Judicial Fugitive Investigation Unit. Both officers had completed a course titled “Managing Sex Offenders’ Computer Use: A 2-Day Technical Training for Probation and Parole Officers.”

The no-cost course, offered at 10 sites per year through the National Law Enforcement and Corrections Technology Center (NLECTC)–Rocky Mountain in Denver, Colorado, provides a comprehensive set of skills and tools for parole and probation officers to manage and monitor offenders’ behavior on the Internet, identify parole violations, and prevent the commission of future crimes. NLECTC–Rocky Mountain is a program of the Office of Justice Programs’ National Institute of Justice. The course also is offered approximately once a year in Colorado through the American Probation and Parole Association.

The success of this course program is being seen in the field, says Jim Tanner, one of the course instructors at NLECTC–Rocky Mountain. Tanner says he has been receiving reports from his graduates who are preventing convictions resulting from their new skills. Two of those success stories come from Stallworth and Newby.

Stallworth participated in the course several years ago. As part of the course materials, he received a disc with software that enables an officer to search the hard drive of an offender’s computer.

After the successes Newby had using his training from “Managing Sex Offenders’ Computer Use,” he arranged to bring the course to his department.

“On the road and offered at no cost to any agency or group of agencies with access to a computer lab and a commitment to implementing a computer monitoring program. More than 440 officers in 16 States have taken the training already, he adds.

In a note of appreciation to NLECTC–Rocky Mountain, Stallworth says: “The offender has finally been adjudicated on these new charges and received a 5-year Federal sentence in conjunction with the State time he was already facing. I felt it necessary to inform you of the fruits of your work and efforts. Thank you, so much. Since your training and the arrest of this offender, I have been favorably called upon statewide to provide training in the supervision of sex offenders. The children of Tennessee and many other states are safer as a result of your diligence.”

Newby adds that in another case, “the man had completely denied having any involvement in the crime [child molestation], or any interest in teens. The raw scan feature of the Field Search program turned up visits to a lot of teen-oriented, really nasty, websites on his computer. He had used ‘wiping’ software to avoid detection, but Field Search was able to track the usage.”

Newby reported that he had immediate success using the new Field Search software.

“The software is great,” Newby says. “[Using the Field Search software] I was able to detect that a sex offender was looking at porn. My previous attempt to detect porn usage by the sex offender failed. I went back with the Field Search software and, after conducting a ‘raw scan,’ I hit the jackpot and found hundreds of pornographic URLs that he had visited.

“To make a long story short, the sex offender then failed his polygraph and will now be sent back to the State of Minnesota, where he transferred from. This software made it possible to detect his behavior, which was a violation of the conditions of supervision, when the other software I had been using failed. The software has helped make our community safer.”

Newby adds that in another case, “the man had completely denied having any involvement in the crime [child molestation], or any interest in teens. The raw scan feature of the Field Search program turned up visits to a lot of teen-oriented, really nasty, websites on his computer. He had used ‘wiping’ software to avoid detection, but Field Search was able to track the usage.”

The success of this course program is being seen in the field, says Jim Tanner, one of the course instructors at NLECTC–Rocky Mountain. Tanner says he has been receiving reports from his graduates who are preventing convictions resulting from their new skills. Two of those success stories come from Stallworth and Newby.

Stallworth participated in the course several years ago. As part of the course materials, he received a disc with software that enables an officer to search the hard drive of an offender’s computer.

Following the training, I used this disk and searched an offender on my caseload and found images of child porn,” Stallworth says. The district attorney and the sex crimes unit of the Metropolitan Nashville Police Department were called in, and the offender’s drives were seized and searched. More than 60,000 images of child pornography were found in the drives and software belonging to this offender. Many of the images appeared to have been taken by the offender in his residence.

Because technology is always evolving, NLECTC–Rocky Mountain regularly updates course materials to stay current. The course has always provided software for the officers to use in their cases, but center staff recently developed freeware specifically for parole and probation officers to use when investigating an offender’s computer. The program, called Field Search, has been part of the training since September 2005 and is proving very effective.

Stallworth says he replaced his older program with the Field Search software and has had tremendous success. “I love Field Search. I have used it for seven or eight searches and all of them have turned up parole violations. In addition, the reports are absolutely wonderful. I can use them in court. I can e-mail them, or I can keep them in my files to provide a full printout of exactly what has been done on a specific offender’s computer.”

Newby reported that he had immediate success using the new Field Search software.

“The software is great,” Newby says. “[Using the Field Search software] I was able to detect that a sex offender was looking at porn. My previous attempt to detect porn usage by the sex offender failed. I went back with the Field Search software and, after conducting a ‘raw scan,’ I hit the jackpot and found hundreds of pornographic URLs that he had visited.

“To make a long story short, the sex offender then failed his polygraph and will now be sent back to the State of Minnesota, where he transferred from. This software made it possible to detect his behavior, which was a violation of the conditions of supervision, when the other software I had been using failed. The software has helped make our community safer.”

According to Joe Russo, program manager for corrections at NLECTC–Rocky Mountain, the course is very hands on. Trainers bring in the computers of actual offenders, who are not identified, allowing officers to use the software in real situations.

The software is great,” Newby says. “[Using the Field Search software] I was able to detect that a sex offender was looking at porn. My previous attempt to detect porn usage by the sex offender failed. I went back with the Field Search software and, after conducting a ‘raw scan,’ I hit the jackpot and found hundreds of pornographic URLs that he had visited.

“On the road and offered at no cost to any agency or group of agencies with access to a computer lab and a commitment to implementing a computer monitoring program. More than 440 officers in 16 States have taken the training already, he adds.

The success of this course program is being seen in the field, says Jim Tanner, one of the course instructors at NLECTC–Rocky Mountain. Tanner says he has been receiving reports from his graduates who are preventing convictions resulting from their new skills. Two of those success stories come from Stallworth and Newby.

Stallworth participated in the course several years ago. As part of the course materials, he received a disc with software that enables an officer to search the hard drive of an offender’s computer.

Following the training, I used this disk and searched an offender on my caseload and found images of child porn,” Stallworth says. The district attorney and the sex crimes unit of the Metropolitan Nashville Police Department were called in, and the offender’s drives were seized and searched. More than 60,000 images of child pornography were found in the drives and software belonging to this offender. Many of the images appeared to have been taken by the offender in his residence.

Because technology is always evolving, NLECTC–Rocky Mountain regularly updates course materials to stay current. The course has always provided software for the officers to use in their cases, but center staff recently developed freeware specifically for parole and probation officers to use when investigating an offender’s computer. The program, called Field Search, has been part of the training since September 2005 and is proving very effective.

Stallworth says he replaced his older program with the Field Search software and has had tremendous success. “I love Field Search. I have used it for seven or eight searches and all of them have turned up parole violations. In addition, the reports are absolutely wonderful. I can use them in court. I can e-mail them, or I can keep them in my files to provide a full printout of exactly what has been done on a specific offender’s computer.”

Newby reported that he had immediate success using the new Field Search software.

“The software is great,” Newby says. “[Using the Field Search software] I was able to detect that a sex offender was looking at porn. My previous attempt to detect porn usage by the sex offender failed. I went back with the Field Search software and, after conducting a ‘raw scan,’ I hit the jackpot and found hundreds of pornographic URLs that he had visited.

“On the road and offered at no cost to any agency or group of agencies with access to a computer lab and a commitment to implementing a computer monitoring program. More than 440 officers in 16 States have taken the training already, he adds.

The success of this course program is being seen in the field, says Jim Tanner, one of the course instructors at NLECTC–Rocky Mountain. Tanner says he has been receiving reports from his graduates who are preventing convictions resulting from their new skills. Two of those success stories come from Stallworth and Newby.

Stallworth participated in the course several years ago. As part of the course materials, he received a disc with software that enables an officer to search the hard drive of an offender’s computer.

Following the training, I used this disk and searched an offender on my caseload and found images of child porn,” Stallworth says. The district attorney and the sex crimes unit of the Metropolitan Nashville Police Department were called in, and the offender’s drives were seized and searched. More than 60,000 images of child pornography were found in the drives and software belonging to this offender. Many of the images appeared to have been taken by the offender in his residence.

Because technology is always evolving, NLECTC–Rocky Mountain regularly updates course materials to stay current. The course has always provided software for the officers to use in their cases, but center staff recently developed freeware specifically for parole and probation officers to use when investigating an offender’s computer. The program, called Field Search, has been part of the training since September 2005 and is proving very effective.

Stallworth says he replaced his older program with the Field Search software and has had tremendous success. “I love Field Search. I have used it for seven or eight searches and all of them have turned up parole violations. In addition, the reports are absolutely wonderful. I can use them in court. I can e-mail them, or I can keep them in my files to provide a full printout of exactly what has been done on a specific offender’s computer.”

Newby reported that he had immediate success using the new Field Search software.

“The software is great,” Newby says. “[Using the Field Search software] I was able to detect that a sex offender was looking at porn. My previous attempt to detect porn usage by the sex offender failed. I went back with the Field Search software and, after conducting a ‘raw scan,’ I hit the jackpot and found hundreds of pornographic URLs that he had visited.

“On the road and offered at no cost to any agency or group of agencies with access to a computer lab and a commitment to implementing a computer monitoring program. More than 440 officers in 16 States have taken the training already, he adds.
A firefighter approaches a burning building ... an emergency medical services crew ... reaches victims of an accident involving a chemical spill ... a law enforcement officer investigates the opening of a suspicious package filled with powder. Foremost on their minds: whether their respiratory equipment is working properly and providing the protection they need to stay alive.

In 1999—2 years before the equipment needs of emergency responders were brought to the forefront by the events of September 11, 2001—the Federal Government initiated a program to coordinate the development and implementation of standards and testing programs for the protective equipment emergency responders need in incidents involving chemical, biological, radiological, nuclear, or explosive (CBRNE) devices.

Congress directed the Office of Justice Programs' National Institute of Justice (NIJ) to do this work under the Anti-Terrorism and Effective Death Penalty Act of 1996. NIJ funded the National Institute of Standards and Technology (NIST) Office of Law Enforcement Standards (OLES) to do the work in accordance with the task prioritized by the Interagency Board for Equipment Standardization and Interoperability. OLES established the First Responder CBRNE Personal Protective Equipment Standards Development Program. Although the program initially focused on chemical and biological protective equipment, it was later expanded to include work on radiation and explosives detection and decontamination.

"In the event of an incident involving CBRNE agents or weapons, first responders need adequate protection so they can help victims without becoming victims themselves," says program manager Phil Mattson, who joined the project in 2001. "This initiative, which strives to establish minimum standards of performance, quality, and reliability, and then test equipment to determine if it complies with the standards, was incorporated into OLES' Critical Incident Technologies Program in 2002.

The program was subsequently transferred to the U.S. Department of Homeland Security from NIJ. "The program continued without missing a beat," Mattson says. "You probably can't say that about too many programs."

Whether NIST is working on standards for respirators, radiation detectors, or bomb suits, the basic approach is the same: determine a reasonable threat level that first responders might face, using studies and modeling. In the case of respirators, for example, the National Institute for Occupational Safety and Health and the U.S. Army Edgewood Chemical Biological Center used extensive modeling to determine reasonable exposure limits for known chemical warfare agents.

"Not surprisingly, many of the respirators on the market failed. The manufacturers simply didn't know what the equipment needed to do," Mattson says, adding that once limits were determined, the manufacturers quickly incorporated results into new models and provided retrofit kits for existing ones.

"But you do have to be careful that you don't set standards that no one can meet." Rather, Mattson explains, "standards should spur development of more effective technologies by quantifying essential performance criteria and establishing communication between equipment users and manufacturers, thus raising both equipment performance and the equipment's user guides. In similar fashion, give first responder agencies important information that will help them make informed purchasing decisions and take proper care of their equipment."

For additional information about the Critical Incident Technologies Program, contact Phil Mattson, 301-975-5396 or philip.mattson@nist.gov. For general information about the National Institute of Standards and Technology or the Office of Law Enforcement Standards, visit www.nist.gov and www.eeel.nist.gov/oles/, respectively.

CBRNE Standards for Law Enforcement and Corrections

Efforts to develop CBRNE (chemical, biological, radiological, nuclear, or explosive) standards have focused primarily on fire services and emergency medical services. Much less attention has been given to developing specific standards for law enforcement and corrections. Phil Mattson, program manager of the Critical Incident Technologies Program at the National Institute of Standards and Technology, believes the time has come to bring the development of standards for law enforcement to the forefront.

"We are ready to develop the requirements; the challenge is to identify the appropriate way to get law enforcement and corrections input so the equipment performs according to the needs of their missions," Mattson says.

Jim Wong, visiting scientist at the Office of Justice Programs’ National Institute of Justice, agrees with Mattson’s assessment: "It’s imperative that we solicit input from the various law enforcement disciplines.

In fact, we recently organized a workshop aimed at defining law enforcement requirements for chemical/biological personal protective equipment ensembles."

Wong says the workshop generated a list of tasks that law enforcement and corrections personnel need to be able to perform while wearing this type of equipment. Input also focused on such areas as wear cycles, exposure times, environmental conditions, and ergonomic requirements.

"Law enforcement has a lot of unique missions, ranging from the routine patrol of the cop on the street to the duties of the bomb squad," Mattson says. "We need their participation and input to make this work."

For more information on efforts by the National Institute of Justice to identify public safety technology needs and requirements, contact Jim Wong at James.Wong@usdoj.gov.
Handling packages that may contain explosives, monitoring restricted drivers, running comprehensive searches of multiple databases, translating languages with a machine, or making a firefighting tool from Austria useful as a less lethal weapon...

On any given day, the Office of Law Enforcement Technology Commercialization (OLETC) in Wheeling, West Virginia, assists inventors and innovators in the development of new products and technologies for public safety agencies large and small.

Here are just five technologies that may soon be helping law enforcement and corrections personnel do their jobs more safely and efficiently.

**Bumping the Bomb Squad**

"Dealing with a package suspected of being a bomb is obviously not a job for the untrained," says Wayne Barte, OLCTE senior project manager. "The bomb technician directs a robot, which crawls along like a fast turtle, to reach the object and then uses a hand-powered tool carried by the robot to work on the object, which could be a box, backpack, pipe under a car, or piece of soft luggage. Naturally, the technician wants to avoid unnecessary delays or problems, such as those caused by a drill that delivers too little torque or a saw that cuts poorly because batteries are running low."

According to Barte, two veteran bomb technicians and members of the Birmingham (Alabama) Police Department designed and patented a "bump" switch to avoid this problem. The switch, an addition to the on-off switching mechanism of a power tool, negates the need to keep a tool turned on while it is being transported to the target. From a safe distance, the technician simply makes the robot bump the switch to turn a tool on when needed and off when not, thus conserving valuable battery power.

OLCTE assistance with this project has included help with developing a commercialization plan and identifying a manufacturer willing to make a small item in small runs for a relatively small market, Barte says. Only a few bump switches exist now, but an adequate supply may be available in a year. Unit cost is expected to be very modest.

**Monitoring Restricted Drivers**

A company's applied-technology division in Virginia is developing a sensing and surveillance system that can monitor drivers whose licenses have been restricted, suspended, or revoked. The License Sanction Enforcement System (LSES™) consists of two parts: the sensors worn continuously by each sanctioned individual and a data-collecting operation run by an LSES contractor. The pair of sensors, strapped to either the wrists or the ankles, detects the distinctive motions associated with driving a vehicle and records the data. The LSES contractor, working in cooperation with law enforcement authorities, periodically downloads the data, which show whether the offender has been driving, and sends it to the appropriate authorities for review.

"The potential benefit of this system is easy to understand," Barte says. "Improved monitoring of sanctioned drivers would directly improve roadway safety. The system would be highly useful to jurisdictions throughout the country, and the offenders could be required to bear the cost of the sensors."

The developer received commercialization assistance through OLCTE's Commercialization Workshop™ and its 24-member advisory council composed of law enforcement experts and scientists. The system, which is not yet perfected or patented, amounts to a product and a service that could be available in a year or two, Barte says. The cost would probably be calculated according to the size of the jurisdiction using the system, but it is too early in the development process to offer a cost estimate.

**Finding With FINDER**

"How important is information sharing to public safety? Consider the case of Mohamed Atta, leader of the September 11 hijackers," Barte says. "On July 5, 2001, Atta was stopped in Palm Beach County, Florida, for speeding and was let go with a warning. A few weeks earlier in neighboring Broward County, police had issued a warrant for his arrest for failure to appear in court on an invalid-license charge, but the police in Palm Beach County had no easy means of checking relevant records in the county next door."

Subsequently, Barte says, the University of Central Florida in Orlando collaborated with the State's sheriffs and police chiefs to design a statewide computer network known as the Florida Integrated Network of Data Exchange and Retrieval (FINDER™). This secure network allows officers to search databases throughout the State and to conduct queries about property, motor vehicles, pawnbroker transactions, and persons and their known associates. An appealing characteristic of FINDER, Barte says, is that it links many data-contributing agencies throughout the region being served while allowing each agency to retain ownership and control of its records. FINDER, a project funded in part by the Office of Justice Programs' National Institute of Justice, is a public partnership governed by a steering committee consisting of representatives from member law enforcement agencies.

After 2 years of testing and evaluation, FINDER is ready to be used by Federal agencies and other States as an information-sharing tool for law enforcement. With OLCTE assistance, the Office of Research and Commercialization at the University of Central Florida has been studying ways to market the copyright-protected software. Barte says the major options are franchising the product to departments of technology transfer at universities in other States or licensing the product to a Fortune 500 company. Whichever option is chosen, he says, the fees charged to subscribing law enforcement agencies will be quite affordable but enough to sustain the FINDER project and fund further development.
Speaking My Language

It is increasingly common today for law enforcement and corrections agencies to communicate with populations that do not speak English well or at all. A single jurisdiction may be home to a variety of peoples, each of which speaks its own language. How are officers of the law to cope with this difficult situation?

In response, Barte says, a Minnesota company has developed a suite of software and hardware products that translates bi-directionally whatever is said, heard, or written. With one product, either user speaks into the device and the words are instantly repeated in the other’s language. It also generates a transcript of the conversation. A second product allows the user to take a picture of a sign, menu, or document and receive a translation in seconds. A third product ensures that the other two provide the same reliable translation.

Development assistance from OLETC included help with commercialization planning and a technology review by the OLETC Advisory Council. A suite of five products is available now; each can be used independently or in any combination with the others, Barte says. The products can run on a personal computer or through a remote server. A basic unit for interactive translation in the field is the size of a small laptop and costs about $1,000.

Watering Down Less Lethal

The Trooper Special Intervention System (SIS) was originally designed by an Austrian company to suppress fires, but the Austrian Special Forces found the device useful as a less lethal weapon. As a firefighting tool, the Trooper SIS discharges a 1-liter blast of water with a muzzle velocity of 500 feet per second, producing water droplets between 50 and 100 microns in diameter, which is a steam-like mass without heat. The blast of the atomized water blows the flames from the surface of the fuel while saturating and cooling the combustible material. The unit weighs about 50 pounds and consists of a short, bazooka-like gun and tanks for compressed air and water.

As a less lethal weapon, Barte says, Trooper SIS can stop an individual or a group of individuals at a distance of up to 7 meters, or 23 feet. For crowd-control purposes, he adds, marking dyes (for identifying individuals later) and chemical agents can be added to the water. Trooper SIS can be used to smash through windows or sheetrock walls when safety concerns rule out pyrotechnic distraction and diversion devices.

The device has been licensed from its Austrian inventor by a Louisiana company, which is emphasizing its potential as a tool for law enforcement and corrections. Likely users would include tactical squads and corrections officers. Barte says, however, that extensive research will be required to determine its precise effects on people when the unit is used as a less lethal weapon.

From OLETC, the company received help with market research and the services of the advisory council. Additionally, the unit was tested during a recent OLETC Mock Prison Riot®. Trooper SIS, Barte says, could be available in a year or so. At present, unit cost is undetermined.

For more information about these and other public safety products and technologies receiving commercialization assistance, contact Wayne Barte, 888-396-5382 or wbarte@uwchf.org. For more information about the commercialization assistance activities offered through the Office of Law Enforcement Technology Commercialization, a program of the Office of Justice Programs’ National Institute of Justice and part of the West Virginia High Technology Foundation Consortium, visit www.OLETC.org.

Principles of Forensic DNA

The Office of Justice Programs’ National Institute of Justice is offering a free, online course on the use of forensic DNA in judicial proceedings.

“Principles of Forensic DNA for Officers of the Court” is a 15-module tutorial developed to educate prosecutors, defense attorneys, and judges on DNA analysis and the legal issues surrounding the use of DNA in the courtroom. Although developed with the criminal justice community in mind, the course, which can be accessed at www.dna.gov, will also interest the general public.

DNA (deoxyribonucleic acid) was first introduced as evidence in the United States in a State court in 1987. DNA technology is now widely used by police, prosecutors, defense counsel, and courts in the United States.

Training modules, which include links to online glossary terms, cover the following topic areas:

- **Introduction.** Provides an overview and program objectives.
- **Biology of DNA.** Discusses biological terminology and the basic biology of forensic DNA identity testing.
- **Practical Issues Specific to DNA Evidence.** Discusses crime scene issues related to DNA evidence.
- **Introduction to the Forensic DNA Laboratory.** Discusses the history of forensic DNA analysis and laboratory processes used in forensic DNA analysis.
- **Assuring Quality in DNA Testing.** Discusses quality assurance and standards that apply to DNA testing.
- **Understanding a Forensic DNA Lab Report.** Provides basic elements and common terminology used in a DNA forensic lab report.
- **Statistics and Population Genetics.** Discusses both the statistical interpretation of DNA evidence and the statistical software used.
- **Mitochondrial DNA & Y-STR Analysis.** Discusses the application of mitochondrial DNA and Y chromosome markers in the examination of biological evidence.

**Forensic DNA Databases.** Discusses how DNA databases can be used to investigate crime.

**Collection of DNA Evidence From a Suspect or Arrestee.** Discusses how a suspect’s DNA is obtained and relevant legal issues.

**Pretrial DNA Evidence Issues.** Covers discovery issues, expert testimony, and defendant issues.

**Victim Issues.** Discusses issues important to victims in cases involving DNA evidence, such as privacy concerns.

**Trial Presentation.** Discusses presentation of DNA evidence to a judge or jury.

**Postconviction DNA Testing Cases.** Discusses legal and procedural issues that should be considered in State postconviction DNA cases.

**Emerging Trends.** Discusses new forensic technologies being developed.

This online training course was developed as part of President Bush’s DNA Initiative, Advancing Justice Through DNA Technology, a 5-year, $1 billion initiative to improve the use of forensic DNA analysis in the criminal justice system through increased funding, training, and other assistance.

For more information about the initiative, visit dna.gov. For more information about the Principles of Forensic DNA for Officers of the Court and other training courses, visit dna.gov/training.
The National Law Enforcement and Corrections Technology Center (NLECTC) system was established in 1994 by NIJ’s Office of Science and Technology to serve as an “honest broker” resource for technology information, assistance, and expertise by providing information and technology assistance to the Nation’s more than 18,000 police departments; 50 State correctional systems; thousands of prisons, jails, and parole and probate departments; and other public safety organizations.

With a network of regional centers and specialty offices located across the country, the NLECTC system delivers expertise in a number of technologies in partnership with a host organization. In addition, a number of technology working groups and a national advisory council provide guidance relating to the technology needs and operational requirements of the public safety community for each of NIJ’s technology focus areas.

Contact NLECTC for:

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 disablement, ordered through NLECTC’s toll-free number, 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 colocated with or supported by federally funded technology partners so they can leverage unique science and engineering expertise.
A Case of Tunnel Vision

In the first 5 months of 2006, authorities discovered at least three tunnels running beneath the California-Mexico border. These underground structures ranged in size and sophistication, with the largest nearly 4,000 feet long. The exit to this almost mile-long tunnel was located inside a large and modern warehouse, a place where tractor-trailers could have loaded illegal narcotics, undocumented immigrants, or even terrorists for transport to any part of the continental United States. According to information compiled by the California Border Alliance Group, 40 tunnels have been discovered nationwide since September 11, 2001, at least 16 of which were in San Diego County. Arizona also has been a site of extensive cross-border tunneling activity. In addition, a tunnel that crossed the U.S. border with Canada was discovered in Linn, Washington.

The Border Research and Technology Center (BRTC) is currently working with the Concepts and Technology Division of the U.S. Department of Defense, Northern Command (NORTHCOM) and the U.S. Department of Homeland Security, Bureau of Immigration and Customs Enforcement field office in San Diego to facilitate demonstrations of potential technology solutions for tunnel detection. BRTC is working with NORTHCOM to define the contents of a possible “tunnel awareness” training module that would help State and local law enforcement be more alert to tunneling activities.

Technologies under study include transmitting low-powered electromagnetic energy to detect subsurface anomalies, using aircraft with special sensors to look for changes in the soil, using instrumented subsurface probes to detect subtle changes in the composition of soil, and detecting the presence of underground water flows that might suggest a tunnel. Different agencies also have examined ground-penetrating radar to confirm the presence of shallow tunnels.

For more information on BRTC’s tunnel awareness initiative, contact BRTC at 888-656-2782 or info@brtc.nleetc.org.

Marshals Get ‘iLinced’

After reading “Getting a TIP. Making a Line” in the Winter 2005 issue of TechBeat (www.justnet.org/techbeat/winter/2005) and learning about iLincs (Intelligent Linked Information Networked Collaboration System), Assistant Chief Deputy Cathy Jones of the U.S. Marshals Service thought it might be just what her agency needed. Responsible for finding a system already proven in the field, Jones contacted the Office of Law Enforcement Technology Commercialization, which in turn set up a meeting and technology demonstration with the help of the Mansfield (Ohio) Police Department. As a result, the Marshals Service launched a 6-month pilot project with a long-term goal of eventually making the tool available throughout the entire agency.

iLincs uses Web-based software and standard computers and Internet connections to provide officers with access to information and photos from both mobile and station-based terminals. The tool enables officers and investigators to retrieve mug shots and jail and court data and create and share field intelligence and alerts complete with photos, fingerprints, and attached documents. Users can also link disparate information sources, build virtual case files, and communicate via e-mail and text messaging.

The Marshals Service began using iLincs in late 2005 and recently decided to extend the project beyond its original 6-month length. For more information, contact Thomas McLaughlin at OLETC, 888-306-5382, ext. 303, or tmlcauglin@oletc.org.

Realizing the Potential of SDR

Software Defined Radio (SDR) holds great potential in addressing public safety challenges such as interoperability and changing radio environments and needs. The Software Defined Radio Forum has released a report titled Software Defined Radio Technology for Public Safety, which presents how SDR technologies can address that potential. The report notes that SDR technology is being implemented in most land mobile radios under development—radios that use technology to support numerous protocols. However, the real promise of SDR for public safety lies in supporting multiband and multisevice radios—radios that could operate with a variety of radio systems and provide ubiquitous interoperability.

Other potential benefits identified in the report include improved performance and reduced life-cycle costs. SDR can improve performance by building smart networks that can adjust to dynamic conditions, including interference and channel loading. Life-cycle costs can be reduced by upgrading functions in software without wholesale system changes and by facilitating migration to new protocols and standards.

The report was written by the forums Public Safety Special Interest Group. The group is chaired by a representative of NJIT’s CommTech Program and includes representatives of the National Public Safety Telecommunications Council, Software Defined Radio Working Group, vendors, software developers, regulators, commercial cellular companies, government and university researchers, and representatives from the CommTech Program and the U.S. Department of Homeland Security. To access the full report, go to www.sdrforum.org/app-docs.html and click on Document No. 2006-4001.

An Undercover Surplus

Thanks in part to NLETC—Southeast, the Illinois Department of Central Management Services (www.cms.dio.gov) has police departments waiting in line to use the five undercover surveillance vehicles that form the core of the department’s recently initiated Equipment Loan Program. The Southeast Center provided technical assistance to obtain and install audio and video recording equipment in the vehicles, which were secured through the Federal Government’s 1033 Program. Additional equipment will be added to the loan program as funding allows.

The Illinois program is modeled after one operated by North Carolina Law Enforcement Support Services, for which NLETC—Southeast also provided startup assistance. The equipment loan program concept requires the State 1033 Program Coordinator’s Office to obtain and maintain, through the 1033 Property Program and other sources, a pool of equipment suitable for law enforcement purposes and make that equipment available on loan to local law enforcement agencies as needed. This pool generally consists of equipment that small local agencies cannot justify purchasing due to cost and/or sporadic need. Examples of other types of equipment available under these programs include trucks, body wires, night vision equipment, and investigative tools.

The 1033 Program (former known as the 200 Program) permits the Secretary of Defense to transfer, without charge, excess U.S. Department of Defense personal property (supplies and equipment) to State and local law enforcement agencies. For more information, contact Ken Dover at NLETC—Southeast, 888-874-5854 or kdover@nleetc-se.org.
of the powered parachutes they were deployed as part of the Hurricane Rita relief efforts in Texas. They were used to survey and photograph damage as well as search for possible looters. The aircraft have also been used to provide aerial photo reconnaissance for the Queen Anne’s County (Maryland) Sheriff’s Office and have been demonstrated to several other Maryland agencies, including the Annapolis Police Department and the Maryland Department of Natural Resources police.

“NIJ is now ready to conduct additional field demonstrations in other parts of the country, and has received inquiries from areas as diverse as Chowan, North Carolina; Moscow, Idaho; and Imperial County, California, in addition to coalitions of agencies on the Savannah River and on the Texas-Mexico Border,” O’Shea says. “Agencies have indicated they would plan to use the craft to look for lost hikers and whitewater rafters, overturned dune buggies, and illicit drug operations and drug smugglers, and to take aerial photos of critical infrastructure such as schools and government buildings.”

In addition to powered parachutes, NIJ is looking at ultralight aircraft and aircraft in the new FAA light sport class. “With the advent of the new FAA light sport class, it is possible for an agency or agencies to own an aircraft that costs from $25,000 to $75,000 and has operating costs of less than $25 an hour, thus meeting the low-cost goal of the NIJ Aviation Technology Program,” O’Shea says.

O’Shea, who soloed on the ultralight craft after about an hour of instruction, says the program has been fortunate to have the volunteer services of Tim Adelman, a Federal Aviation Administration-certified flight instructor. Adelman, a lawyer in the Annapolis area, has been showing NIJ staff members and law enforcement officers how to fly the aircraft. Another boost to the program has come from the owners of Talisman Airstrip on Maryland’s Eastern Shore, who donated storage space and allow free use of the three landing strips.

For more information about NIJ’s evaluation of powered parachutes and its Aviation Technology Program, contact Mike O’Shea, 202–305–7954 or Michael.OShea@usdoj.gov.

Editor’s Note: Any agency considering the use of powered parachutes for law enforcement activities should first consult with its legal advisors and/or contact the Federal Aviation Administration, 866–835–5322. All ultralight operations are covered by Federal Aviation Regulation Part 103. This regulation can be accessed at safetydata.com/afire/seminar4.htm. For additional information about ultralight and light sport aviation, visit www.usua.org.

NATIONAL CRIMINAL JUSTICE REFERENCE SERVICE

In addition to funding the National Law Enforcement and Corrections Technology Center, the National Institute of Justice (NIJ) and other Federal agencies support the National Criminal Justice Reference Service (NCJRS), assisting a global community of policymakers, practitioners, researchers, and the general public with justice-related research, policies, and programs.

NCJRS offers reference and referral services, publications, onsite and offsite conference support, and other technical assistance. The easiest way to access NCJRS is online.

Start at http://www.ncjrs.gov. The NCJRS website showcases the latest criminal and juvenile justice and drug policy information. Take advantage of:

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

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

- JUSTINFO. A biweekly electronic newsletter that includes links to full-text versions of printed publications.
- E-mail notifications. Periodic messages about new publications and resources that match your specific interests.

NCJRS Contact Information at-a-Glance

Web: http://www.ncjrs.gov
Phone: 800–851–3420 (Monday – Friday, 10 a.m. to 6 p.m. e.s.t.)
Fax: 301–519–5212
Mail: NCJRS, P.O. Box 6000, Rockville, MD 20849–6000

The National Law Enforcement and Corrections Technology Center is supported by Cooperative Agreement #2005-MU–CX–K077 awarded by the U.S. Department of Justice, National Institute of Justice. Analyses of test results do not represent product approval or endorsement by the National Institute of Justice, U.S. Department of Justice; the National Institute of Standards and Technology, U.S. Department of Commerce; or Lockheed Martin Aspen Systems Corporation. Points of view or opinions contained within this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

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

tuated in the industrial steel and coal mining area of eastern Pennsylvania is the City of Bethlehem. During the fall of 2005, the city's police department conducted an investigation of graffiti that began popping up in various locations throughout the city. As part of the investigation, department personnel became themselves miners—not miners of coal, but rather miners of data. Their pick and shovel—a data-mining software program recently developed by researchers at Pennsylvania's Lehigh University and in beta testing by the department.

In the investigation the software was able to show links between the words, paint colors, and locations of the graffiti. The suspect responsible was identified along with his gang affiliation, and the investigation lead to multiple arrests on a varied group of charges, including drug violations.

Leveraging funding from the Office of Justice Programs' National Institute of Justice and the National Science Foundation, Lehigh's Dr. William Pottenger and his team worked with the Bethlehem police to create the Bethlehem Police Department Information Extraction System. The system is a data-mining tool that delves into unstructured narrative text and pulls out links between names, birthdates, addresses, vehicles, and the like, helping investigators quickly find any similarities between crimes.

When Pottenger originally came to the department with his proposal, Randy Miller, Bethlehem's deputy commissioner of police, told the professor that the department's historical data existed in a variety of formats, ranging from typewritten reports to microfilm in WordPerfect® and MicroSoft® Word®.

"The problem was, we didn't have the funding or the time to update data from one system to the next," Miller says. "For example, our WordPerfect files still existed on an old server, but we didn't have any software that could access them. Using sophisticated data mining techniques and algorithms, the Lehigh team is now able to take the old records management systems, pick out key words, and make the information accessible.

"This is a common problem faced by police departments. The old information is still good, but it is lost. Fortunately for us, ours is not lost any longer. Now we might find that a string of robberies taken place right now shows the same modus operandi as a string that occurred 10 years ago. Data mining can find the link, and our investigators might learn that the man who committed the previous robberies was just released after serving 10 years in the State prison. They now have a solid suspect," Miller says.

Another example of how the data-mining software could help investigators, explains Miller, is searching records of cold homicide cases for the word “blood.” Finding that word in a 20-year-old case report could indicate the possibility of uncovering DNA evidence that might generate new leads.

"We're getting data and relationships we thought were long lost," he says. "Because of this system, we can view and extract important pieces of data. It fills in a gap that I think all police departments have." He adds, "Investigators get promoted, retire, and move on, and the experience and knowledge about past cases moves on with them, but the data remains. Now, with data mining, it won't be forgotten."

Lehigh's Pottenger, who has been working in data-mining research for several years, became interested in helping law enforcement when he realized the amount of underutilized data collected by most police departments.

"There is a lot of power that can be found in this type of resource," Pottenger says, citing as an example a nationwide methamphetamine bust engineered by the U.S. Department of Justice that used manual collection to link records across the country. "Our goal is to make it possible for law enforcement to do this easily and automatically. Anything that was ever recorded, even if it was just a comment on a form, or even a receipt, could contain valuable information that might link cases."

Pottenger notes that although there are commercial products with similar data-mining capabilities, their licenses tend to be too expensive for many police departments to afford. The project focused on coming up with ways to reduce the "knowledge engineering" cost so as to produce technology that could be marketed for less money. "We're in discussions now about licensing it," Pottenger says. "We've had interest expressed by two or three different law enforcement projects."

In developing the software, which runs on an ordinary personal computer, the Lehigh team consulted with several law enforcement personnel to ensure that the final product is easy to use. The system offers three different search modes: a Google™ type string search interface, a standard form with drop-down menus, and a new-incident search that compares results against the existing database.

With the string interface, Pottenger says, users simply type in the words they want to find and can also qualify them by using a field value such as "Age: 15." The form with drop-down menus allows users to choose terms from one or more categories—for example, the term "father" from the "Relationship" menu. The new-incident search asks users to choose the data they want to match, such as a weapon type. The goal of each search mode is to provide a list of closely matching previous incidents and a short list of suspects.

In a preliminary evaluation of the system, commonly occurring crimes such as theft, malicious mischief, and burglary were used to look for links among modus operandi. Pottenger and his team plan a further evaluation in Florida that will test the system in conjunction with the State’s FINDER system, which tracks pawn transactions. Pottenger plans to mine written narrative police reports for data on stolen items and match these data against the pawn transaction database.

For more information about the Bethlehem Police Department Information Extraction system, contact William Ford at the National Institute of Justice, 202–353–9768 or William.Ford@usdoj.gov; or Dr. William M. Pottenger, 610–758–3454 or DrWMPottenger@gmail.com.
(It’s in the Mail . . . cont. from page 3)

• Solar-powered automatic ventilation system to cool the cargo area in warm weather.

• Security panels for the cargo area (steel mesh inside windows and a solid compartment door with push-button cipher lock) to reduce likelihood of equipment theft.

• Shore power to enable electrical support while parked (with automatic ejection system to disconnect cord when engine is started).

The vehicles are equipped with hazardous materials personal protective equipment and other items such as radiation detectors, gas detectors, and field-screening equipment for powders encountered in the mail. The Inspection Service adapted existing technology to suit its needs.

“We looked at what other first responders, such as fire departments and hazardous materials teams, use to assess unknown substances.” Brinkley says. “We decided not to rely on technology that attempts to identify the material with multiple field assays. In several cases, field testing by other first responders used up all the powder and there was nothing left for a lab to test. We also wanted to avoid false negatives or false positives that are too common with many field assays. We developed our systems to use a tiny amount of material, and instead of attempting to identify the material, we focus on ruling out dangerous substances.”

Protocols are based on the Centers for Disease Control and Prevention (CDC) list of bioterrorism agents, such as anthrax and ricin. The CDC classifies agents with recognized bioterrorism potential into three priority areas. (See www.bt.cdc.gov/agent/agentlist-category.asp for more information.)

Of primary importance is to eliminate a suspicious substance as dangerous. “Inspectors use field screening to rule out the presence of a bioterrorism agent or weapon,” Brinkley says. “We’re not necessarily trying to identify the substance. If it can’t be ruled out as a weapon, or if it is associated with a credible threat, we transport it to a lab for definitive testing.”

“We brought the technology together based on what we encounter in the mail, and it requires more space than what our typical vehicles can handle. We designed the trucks to transport and support the equipment and supplies we need for an effective response, but they really aren’t very different from trucks used by other agencies.”

The Inspection Service also used the vehicles to assist its post-hurricane assessment of conditions of postal facilities during the 2005 hurricane season. The personal protective equipment in the trucks came in handy, and the trucks also carry equipment to check for dangerous fumes.

For additional information on the special response vehicles used by the U.S. Postal Inspection Service, contact Tripp Brinkley, postal inspector/program manager, Dangerous Mail Investigations and Homeland Security Group, 202-268-5088 or TBrinkley@uspis.gov.