A CapWIN-Win Solution

Spanning the Potomac River just south of Washington, D.C., the Woodrow Wilson Bridge handles tens of thousands of vehicles every day. The bridge is part of the I-95 corridor that carries traffic along the East Coast from Maine to Florida and part of the Capital Beltway that carries commuters between their homes and their jobs in Virginia, Maryland, and the District of Columbia.

In 1998, a man threatening to jump from the bridge into the Potomac River closed the bridge for more than 5 hours, bringing traffic in the region to a standstill. Incompatible communications equipment prevented emergency personnel from different jurisdictions on the scene from being able to communicate with each other. This communications gap resulted in confusion and unnecessary delay in resolving the incident and the resulting traffic problems.

Unfortunately, this was not a singular incident. In the Washington, D.C., metropolitan region, public safety personnel responding to a critical incident involving multiple jurisdictions are often hampered by an inability to communicate directly with other agencies.

To address this communications gap, officials from Maryland, Virginia, and the District of Columbia launched the Capital Wireless Integrated Network (CapWIN) in 1999 with initial funding from the U.S. Department of Transportation and the National Institute of Justice’s (NIJ’s) AGILE Program, which helps local and State public safety agencies address interoperability issues.

The goal of the CapWIN project is to create the first integrated multi-State transportation and public safety information wireless network in the United States. Once completed, CapWIN will allow police officers, firefighters, transportation officials, and other emergency personnel to communicate directly with each other during a critical incident using standard laptops. As a result, personnel from different agencies will be able to develop a coordinated response to an incident.

The idea behind the program “is to allow different [public safety and transportation] agencies to communicate and to set up a logical means of doing it,” says John Binks, the CapWIN Training Manager at the University of Maryland’s Center for Advanced Transportation Technology. IBM, the primary integrator on the project, will build the network with off-the-shelf components and provide an open standard interface to allow participating agencies to communicate with each other using their existing equipment. “It’s much better than trying to get three States to throw away all of their equipment and [then] spend more money on the same type of equipment,” Binks says. CapWIN also will provide mobile computing capabilities for agencies that currently have none.

Using a standard laptop mounted in a police cruiser or a fire truck, users will be able to log on to the CapWIN system using a Web browser. Once logged on to the network, they will be able to see which other agencies are logged on using a global directory, instant-message those other users, or enter chat rooms set up for a specific incident to find out the latest information.

Law enforcement users will be able to use CapWIN to access crime databases in all three jurisdictions, which, Binks says, is “groundbreaking . . . . It’s a big deal to have three different States working together” and sharing sensitive information. Typically, when a police officer pulls over a car and runs a check on the driver’s identification, the officer is able to obtain information only from the National Crime Information Center, which is a national crime database, and the crime database in his or her jurisdiction. The officer

Making Way for Segway

They’re called Human Transports (HTs) and they’ve been featured on the news, advertised on Internet popup ads, and more and more, seen on city streets carrying a courier or a postal delivery person. But with the assistance of the National Institute of Justice’s (NIJ’s) National Law Enforcement and Corrections Technology Center (NLECTC) system, Segway HTs may become standard issue for law enforcement and corrections officers.

“Segway is looking at different applications where the devices could be tested, applications where people wear or carry a lot of heavy gear. That includes Army special operations as well as law enforcement bomb squads and HAZMAT teams,” says Bruce Richter, program manager at NLECTC–Northwest in Anchorage, Alaska. In turn, he says, law enforcement officers are interested in using the transporters in such areas as parks, parking garages, and crowded downtown streets.

Early in 2003, Michael O’Shea, NIJ’s program manager for NLECTC–Northwest and a former law enforcement officer, contacted Segway regarding its evaluation program. In May, the company sent a representative to Anchorage to demonstrate the device. Shortly thereafter, NLECTC–Northwest was given the green light from its advisory council to be part of the evaluation program. In August, 10 officers from the Juneau Police Department received training on two Segways provided on loan by NLECTC–Northwest.
Initially, Richter had reservations. But he quickly realized the battery-operated vehicles presented a number of advantages. “It looks like a toy, so you don’t realize its capabilities,” he says. “Then, when I saw the photographs of bomb suit testing, it instantly clicked. Bomb suits sometimes can weigh about 100 pounds, and they’re hot. They wear you out quickly. The Segway can get you on the scene quickly, extend your available work time, and get you away quickly. It just made sense.”

Richter also notes that officers on Segways wearing HAZMAT airpacks do not use up their air supply as quickly as they would if they walked to a scene, that type of physical exertion often lags up face masks, another potential problem avoided by Segway use. Because all the electronics on a Segway HT are sealed, it can be quickly decontaminated by washing it down after use at a HAZMAT scene.

“It has many uses for people who have to be on their feet in areas that are congested with people, such as narrow hallways and crowded streets,” says Maxine Andrews, also a program manager at NLECTC–Northwest and one of three Segway HT-certified trainers on the center’s team. “It respects the environment, since there are no emissions. It doesn’t take months to learn how to use. I helped train the officers in Juneau, and they were out on the street patrolling almost immediately. The evening of the training, they went out and took it up the steepest hill they could find to check its performance.”

Alaska law enforcement agencies quickly caught on to Segway’s potential. Although the Juneau police filed the first application to participate in the Segway loaner program, after just 1 month of operation, NLECTC–Northwest had already received numerous other requests, including—

■ Alaska State Department of Corrections for correctional facility interior patrol.

■ Several large high schools for school resource officer campus patrol.

■ Alaska State Troopers for parking lot patrol at the State fair.

■ Ted Stevens International Airport in Anchorage for parking garage and terminal patrol.

■ Law enforcement agencies on the islands of Kodiak and Sitka for patrol.

All of these agencies, and others, lined up to borrow the Segway HTs, Andrews says. “One agency may try them and say, we have no use for them, and the next will say, yes, we want to buy them. Either way, they haven’t had to spend money to find that out.”

Juneau P.D. started the process by borrowing two of the three NLECTC–Northwest Segway HTs from August to October 2003. Richter says that up to five cruise ships, each carrying as many as 3,400 passengers, may dock in Juneau at the same time. “That creates so much foot traffic, it’s hard to get a police cruiser through if there is an incident near the docks. Another advantage is that officers using the devices stand about 8 inches taller than others in a crowd, providing them a much better view of their surroundings.”

While Juneau had two Segways to test, a third moved around to other interested agencies. However, no agency gets a Segway until officers from the agency take a formal 4-hour training course on its use.

“Training is designed to give you the tools to understand the capabilities of the machine and help you avoid the ways that you can get yourself into trouble with it.” Richter says. “It’s easy enough to get a false sense of confidence after using it for only a few minutes; you think you know how to move it. What you really know is just enough to get yourself into trouble.”

Richter says problems commonly encountered include maneuvering too close to an object—so the sidewalk runs up against it and the Segway attempts to climb the object—or trying to turn too quickly, given its tight turning radius.

“After officers take the training, they become extremely excited after seeing what the devices can do,” Andrews says. “They might have thought they couldn’t use it, but now they can see all kinds of applications. For example, you could use it to patrol at a street fair and not be exhausted from walking if, late in a shift, you’re called on to give chase. You also could be at one end of that street fair, or at one end of an airport, and get a call that a defibrillator is needed at the other end.” According to Andrews, early reports from officers at Anchorage’s airport show that an officer carrying such equipment on a Segway could beat officers on foot to the other end of the terminal by as much as 2 minutes—critical time for someone suffering a heart attack—and arrive with plenty of “wind” to start CPR, if necessary.

Segway HTs have a range of about 12 miles on currently available batteries. “We don’t expect an officer to typically use it for an entire shift, just for a few hours here and there,” Richter says. The device needs about 4 to 6 hours for a complete recharge. Lithium batteries, which will be available soon, will double the range of the device. Another enhancement that already is available is an all-terrain tire, which could improve winter operation. However, many of the Alaska agencies appear more interested in using it indoors than in deep snow, and coastal areas like Juneau typically receive more rain than snow. He says that agencies interested in buying their own Segways after trying out the NLECTC–Northwest loaners can apply for U.S. Department of Homeland Security grant funds to pay for the devices, which cost around $5,000 each.

In addition to police and corrections agencies in Alaska, evaluations of Segways arranged through NIJ and the NLECTC system have been conducted by police departments in Annapolis and Montgomery County, Maryland, and Syracuse, New York, and by the sheriff’s department in Los Angeles County, California, for the local transit system. The device also will be evaluated by Port Authority Police at John F. Kennedy International Airport in New York and by school safety officers across the country.

For more information on the Segway Human Transporter loaner and evaluation program in Alaska, contact Bruce Richter at bruce.richter@ctsc.net or Maxine Andrews at maxine.andrews@ctsc.net. Both can be reached by telephone at 866–569–2969. For more information about the program elsewhere in the United States, contact Michael O’Shea, 202–305–7854 or osheam@ojp.usdoj.gov.
may find no outstanding warrants for the person in
that State. CapWIN will allow the officer to view the
crime databases in all three jurisdictions, potentially
alerting the officer that the person is wanted in an-
other State. Binks says the agencies determine how
much information they want to share from their data-
bases and who can access it. According to NIJ
program manager Tom Coty, agencies will be
sharing “even hot files with each other like
warrants and criminal records, and other
information they normally wouldn’t share.”
As a result, CapWIN “will provide much more
powerful information for any participating
agency in the D.C. area,” which will make
police officers “safer and more informed,”
Coty says.

To date, CapWIN has already proved
on a small scale that it can do what it was
designed to do. In 2001, project staff con-
ducted a pilot project in which 22 laptops
were mounted in police, transportation, and
fire vehicles in the 3 jurisdictions to deter-
mine if messaging between the vehicles was
possible. Says Binks, “The idea was to see
if we could get some limited technology to
communicate back and forth.” With the use
of the Alexandria (Virginia) Police
Department’s messaging switch, the vehicles
were able to interface and transfer
information from one agency to another.

The next step in the process, according to Binks,
is to conduct beta testing to learn which aspects of
the network are working well and which need to be
modified. In fall 2003, personnel from 16 agencies in
the region received training at the CapWIN Training
Center on how to use the CapWIN network interface.

Next, Binks says CapWIN plans to put 56 laptops in
vehicles in target areas for about 3 months of testing.
After testing is completed, Binks says the project will
be ready to go into full production.

In addition to beta testing, Binks says CapWIN and
IBM are working on an interface for PDAs (personal
digital assistants). This interface will allow motorcycle
police, police on foot patrols and horseback, and
police in helicopters to use PDAs as officers in patrol
cars will use laptops—to access criminal databases
and run background checks or send instant-messages
to personnel from another agency. Binks says local
agencies have already been asking about the PDA
interface “pretty aggressively.”

Currently, he says about 35 agencies in the D.C.
metropolitan region are involved with CapWIN.
He expects that number to grow because CapWIN
receives daily inquiries about the project and staff
are invited to appear at conferences across the Nation
to speak about the project. For agencies in the D.C.
metropolitan area that are interested in becoming
involved with CapWIN, Binks says, “All they have to
do is call us.”

NIJ’s Coty predicts that, if successful, CapWIN
will have national implications. “What we will get
out of this is a model that can be replicated, that
details how to develop the partnerships and coop-
eration among the many different agencies, and
that leverages as much of the existing technology
as possible.” Binks adds that a requirement of the
CapWIN project is to develop a national model that
other States can adopt. To that end, a full-time stan-
dards manager is responsible for providing doc-
umentation on everything the project has
done so it can be easily replicated. Says
Binks, “That’s the unique aspect of
coming through a university and
being grant funded. People can learn
from what we’ve done.” He adds,
“We’re not selling anything, we’re
trying to solve a problem.”

For more information about the
Capital Wireless Integrated Network project,
call 301–614–3700 or visit the CapWIN website
at www.capwin.org. Or, contact Tom Coty at
the National Institute of Justice, 202–514–7683;
cotyt@ojp.usdoj.gov.
Since the information technology revolution began, law enforcement has faced the growing problem of cybercrime. But a lack of resources and trained personnel has put many agencies behind the curve. Along with trained personnel to investigate such traditional crimes as murder, arson, theft, and assault, law enforcement needs “cyber cops” to fight electronic crime.

“Traditional crime is a lot different than cybercrime,” says NLECTC–Northeast’s Robert DeCarlo, Jr., who is an economic crime specialist with CSL. “Some of our investigators are former police officers. But cybercrime is a unique opportunity to gain knowledge and hands-on experience in the field of cyber security in the law enforcement community.”

The foundation of this program is a joint venture between academia and both the public and private sectors in an effort to expose students to a challenging experience in support of cyberscience developments.

“One of the things that I like to emphasize is that we’re trying to help these young people find productive, meaningful jobs,” DeCarlo says. “We want to get them involved in the area of e-crime and encourage them to make it their specialty in law enforcement or private industry, as a computer forensics analyst or similar occupation. The goal is to get them involved in the field and have them stay in it.”

DeCarlo explains that CSL creates internships in which “students do more than fill papers. They perform full-time, productive work, which could include heading up a special project or making a key presentation. Projects vary according to CSL’s needs but often include testing and tool assessments.”

“For example,” DeCarlo says, “one of the interns [Roseanne Comito] who I mentored tested a steganography detection tool . . . . She wrote a detailed assessment for the vendor and the vendor used it to refine the tool.” (Steganography is the art of hiding data within a computer graphic or file.) Comito used her knowledge of steganography on another project, working with a group of gifted middle school students who were part of the Discovery Channel’s 2002 Young Scientist Challenge competition. [Editor’s note: More information about Roseanne Comito’s project and the Young Scientist Challenge can be found at http://access.ncsa.uiuc.edu/Stories/Detectives/.]

Comito’s project involved middle school students. But another CSL internship program conducted during summer 2003 offered high school students workplace experience and allowed them to create a course about cybercrime for other high school students. “They talked to the staff and get a feel for the workplace,” says Andrea Belmont, an electronic crime specialist with CSL. “They chose to create a website to showcase the course,” which focuses on information assurance and cybersecurity, or ways to protect network data and systems.

Both the high school and college interns receive wages based on their experience, DeCarlo notes. This experience plays a key role in whether they are selected to participate in the program. He says that he, Belmont, and others review the resumes submitted each semester and select qualified students.

“Sometimes we look at resumes,” DeCarlo says, “we primarily look for someone who is studying criminal justice, information technology, or computer science; who is interested in cybercrime; and who wants to stay in the field as a career.” Belmont adds that although there is no set grade-point standard, students must be in good academic standing and receive a recommendation from an instructor. Many applicants learn about the internship program from their instructors who urge them to apply.

Schools that have participated in the internship program include Utica College, Syracuse University, University of Miami, Florida Atlantic University, George Mason University, Carnegie Mellon University, Dartmouth College, Stanford University, State University of New York Institute of Technology, Hilbert College, Cornell University, Columbia University, and John Jay College of Criminal Justice. DeCarlo points out that interns do not have to relocate to upstate New York for a semester. CSL can place interns with U.S. Secret Service e-crime task forces across the country. DeCarlo says that any college that would like to take part in the program should call him. “We’ll talk and figure out if they have programs we can draw from.”

To find out more about the CyberScience Laboratory e-Crime Intern Program, contact Robert DeCarlo, Jr. at 888–338–6584 or e-mail robert.decarlo@rl.af.mil.
### TERMS

<table>
<thead>
<tr>
<th>TERMS</th>
<th>DEFINITIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Steganography</td>
<td>a. A unique string of numbers that identifies a computer or device on the Internet.</td>
</tr>
<tr>
<td>2. Firewall</td>
<td>b. A malicious program that masquerades as a benevolent one.</td>
</tr>
<tr>
<td>3. Trojan Horse</td>
<td>c. A type of network in which individual users connect to each other directly, without a centralized server. Can be used to share files (legal or illegal) easily among individuals.</td>
</tr>
<tr>
<td>4. IDS (Intrusion Detection System)</td>
<td>d. The art of hiding data or pictures within a file or files.</td>
</tr>
<tr>
<td>5. Network Sensor</td>
<td>e. The act of capturing packets of data flowing across a computer network.</td>
</tr>
<tr>
<td>6. Peer-to-Peer (P2P) Network</td>
<td>f. An attack that seeks to slow or disable a network by overwhelming it with useless traffic.</td>
</tr>
<tr>
<td>7. Information Assurance</td>
<td>g. The protection of data and systems in networks connected to the World Wide Web.</td>
</tr>
<tr>
<td>8. Cybersecurity</td>
<td>h. A system that scans areas within a computer or network for possible security breaches.</td>
</tr>
<tr>
<td>9. IP Address</td>
<td>i. The act of deceiving people into divulging information that allows access to computers and network infrastructure.</td>
</tr>
<tr>
<td>10. E-mail Spoofing</td>
<td>j. The protection of information systems to ensure their integrity.</td>
</tr>
<tr>
<td>11. Denial of Service (DoS)</td>
<td>k. A set of related programs that protect a private network from users based outside the network.</td>
</tr>
<tr>
<td>12. Social Engineering</td>
<td>l. A program that monitors or “sniffs” a system for problems.</td>
</tr>
<tr>
<td>13. Packet Sniffing</td>
<td>m. The act of forging the header information on an e-mail so that it appears to have originated from somewhere other than its true source.</td>
</tr>
</tbody>
</table>

---

**5th Annual Innovative Technologies for Community Corrections Conference**

**June 14–16, 2004**

Fairmont Copley Plaza • Boston, Massachusetts

**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
- Drug and Alcohol Testing Technologies
- E-Learning for Community Corrections
- Advances in Electronic Monitoring
- Technology to Manage Sex Offenders
- 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.
A Disaster Waiting To Happen

When the Federal Emergency Management Agency (FEMA) published a list of disaster preparedness training objectives in the wake of the attacks of September 11, 2001, chances are the agency did not envision that it would result in 72 hours of mass casualties and terrorist threats.

Conversely, on an early September weekend in mid-Ohio Valley, Moundsville, West Virginia, faced a domestic terrorist drug laboratory, a suspicious package, a natural disaster, a mass casualty event, and more. For the second time in a year, Moundsville was in the midst of a series of incidents that would tax public safety agencies to their limits.

First, Ohio Valley town and surrounding area was hit all just part of Mock Disaster 2002, sponsored by the National Commission on Law Enforcement and Technology Center (NCLETTC). NCLETTC, located in Moundsville, was established as a year-round training and technology center for corrections, law enforcement, and public safety.

The September 2002 event was the second mock disaster organized by the center with assistance from the National Institute of Justice’s Office of Law Enforcement Technology Communication and the National Technology Transfer Center’s Emergency Response Technology Program, both in nearby West Virginia, National Corrections and Law Enforcement Technology Program, which hosted the 3-day mock disaster. The planning committee—which included local, state, and federal law enforcement, hospitals and health departments, fire departments, environmental correctional agencies, medical examiners, and local chemical companies—would have to improvise on the spot.

“This disaster” began and ended with the informant: a phone call about illegal activities at ‘Acme Environmental Labs,” then the recovery of a barrel full of “remains” from the river. In reality, the barrel contained a number of body parts in pieces too small to identify (DNA from cells later identified them as the informants). And the other contained “suspicious substances.”

The next morning the arrival of a suspicious package at the local wastewater treatment plant pulsed city police, fire, and rescue agencies to one side of town. Recognizing that they lacked the proper equipment and resources, the local agencies called in an explosive response team from the West Virginia State Police. Meanwhile, across town on a local park, an ambulance arrived: the “patient” had been transferred on a stretcher to another hospital. The two incidents became part of a complex series of scenarios that would take on a life of their own.

The “disaster” began and ended with the informant: a phone call about illegal activities at “Acme Environmental Labs,” then the recovery of a barrel full of “remains” from the river. In reality, the barrel contained a number of body parts in pieces too small to identify (DNA from cells later identified them as the informants). And the other contained “suspicious substances.”

The next morning the arrival of a suspicious package at the local wastewater treatment plant pulsed city police, fire, and rescue agencies to one side of town. Recognizing that they lacked the proper equipment and resources, the local agencies called in an explosive response team from the West Virginia State Police. Meanwhile, across town on a local park, an ambulance arrived: the “patient” had been transferred on a stretcher to another hospital. The two incidents became part of a complex series of scenarios that would take on a life of their own.

The agencies taking part in the six scenarios included emergency medical services, fire departments, law enforcement and corrections agencies, 911 centers, hospitals, medical examiners—offices, the Federal Bureau of Investigation, the U.S. Armed Forces, the Salvation Army, utility companies, local industries—even a hospice. Park recalls her surprise when she learned that a local hospice wanted to join in the drill. She learned that after September 11, hospice agencies took on baverage counseling following mass deaths. Because the scenarios included multiple fatalities, the hospice would need to provide counseling.

We look at them all, and said it’s true that this is real life as possible,” Park says. “While it’s all true to this type of drill in rural West Virginia, when you step up and think about it, we have the Ohio River right here, we have Interstate 70 coming through the area, and it’s really quite feasible. We’re talking West Virginia, and we’re also talking rural United States. This is how most of us live and work. Most of us don’t live in large cities.

The mock disaster planners had to do more than develop the six scenarios. They also drew up plans for the workshops and vendor demonstrations that would be held during the 3-day event. Workshops, Park says, ranged from “Terrorist ID for Everyday People” (how to help mail carriers, meter readers, and others identify suspicious behavior) to “Rope Rescue Operations for the Emergency Responder.” Participants had 24 workshop reasons to choose from, of which were offered twice.

Participants also could visit approximately 50 vendor booths displaying new technologies. Prior to the event, the planning committee reviewed the technologies to be displayed and selected vendors for use in particular scenarios. For example, a thermal imaging camera was made available for evidence collection in a warehouse.

At this technology did not fit into a scenario, vendors could demonstrate their products in a scheduled session. Technologies and demonstrated included chemical detection systems, personal alarms, a smoke generator for use in firefighter training, gear to protect first responders from extreme heat, respiratory protection gear, thermal vision gear, and incident monitoring software.

The planning committee reviewed the technologies to be displayed and selected vendors for use in particular scenarios. For example, a thermal imaging camera was made available for evidence collection in a warehouse.
The National Law Enforcement and Corrections Technology Center (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.

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.

With a network of regional centers and specialty offices located across the country, the NLECTC system has been able to deliver expertise in a number of technologies by forming partnerships with such host organizations as the Air Force Research Laboratory, the Space and Naval Warfare Systems Center, and The Aerospace Corporation. Through these partnerships, NLECTC staff have access to the latest innovations in research and development.

The NLECTC system serves as an “honest broker” resource for technology information, assistance, and expertise.

Contact NLECTC for:

Technology Identification
The NLECTC system provides information and assistance to help agencies determine the most appropriate and cost-effective technology to solve an administrative or operational problem. We deliver information relating to technology availability, performance, durability, reliability, safety, ease of use, customization capabilities, and interoperability.

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 Implementation
We develop technology guides, best practices, and other information resources that are frequently leveraged from hands-on assistance projects and made available to other agencies.

Property Acquisition
We help departments take advantage of surplus property programs that make Federal excess and surplus property available to law enforcement and corrections personnel at little or no cost.

Equipment Testing
In cooperation with the Office of Law Enforcement Standards (OLES), we oversee the development of standards and a standards-based testing program in which equipment such as ballistic- and stab-resistant body armor, double-locking metallic handcuffs, and semi-automatic pistols is tested on a pass/fail basis. NLECTC also conducts comparative evaluations—testing equipment under field conditions—on patrol vehicles, patrol vehicle tires and replacement brake pads, and cut-, puncture-, and pathogen-resistant gloves. NLECTC also has evaluated emerging products to verify manufacturers’ claims. The primary focus of OLES is the development of performance standards and testing methods to ensure that public safety equipment is safe, dependable, and effective.

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), Operation America (bomb detection technologies), and an annual public safety technology conference. On a limited basis, NLECTC facilitates deployment of new technologies to agencies for operational testing and evaluation.

Capacity Building
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, in-mate disturbances and riots, and computer crime investigation.

Technology Information
NLECTC disseminates 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)

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 comprised of five regional centers and is complemented by several specialty offices and a national center. Most centers and offices are co-located with or supported by federally funded technology partners so they can leverage unique science and engineering expertise.

the ‘center system’

The NLECTC–National
2277 Research Boulevard Rockville, MD 20850 800–248–2742 asknlectc@nlectc.org

The NLECTC–Northeast
26 Electronic Parkway Rome, NY 13441–4514 888–338–2742 nlectc_northeast@fbi.gov

The NLECTC–Southeast
5300 International Boulevard North Charleston, SC 29418 800–292–4385 nlectc_seo@nlectc-sa.org

The NLECTC–West
888–548–1618 nlectc@law-west.org

The NLECTC–Northwest
888–548–1618 nlectc_nw@ctsc.net

Border Research and Technology Center (BRTC)
1010 Second Avenue, Suite 1920
San Diego, CA 92101–4912
888–656–2782
info@brtc.nlectc.org

Rural Law Enforcement Technology Center (RULETC)
101 Bulldog Lane
Hazard, KY 41701
866–787–2553
ruletc@fbi.gov

Office of Law Enforcement Standards (OLES)
109 Bureau Drive
Gaithersburg, MD 20899–8102
301–838–1500
oles@just.gov
Offered through JUSTNET, the website of NLECTC, this weekly news summary provides synopses of recent articles relating to technology developments and initiatives in law enforcement, corrections, and the forensic sciences that have appeared in newspapers, newsmagazines, and trade and professional journals. The summaries also are available through an electronic e-mail list, JUSTNETNews. Each week, subscribers to JUSTNETNews receive the summary directly via e-mail.

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

Note: Providing synopses of articles or mentioning specific manufacturers or products does not constitute the endorsement of the U.S. Department of Justice or NLECTC. Reproduction of this text is encouraged; however, copies may not be sold. The NLECTC Law Enforcement and Corrections Technology News Summary should be cited as the source of the information. Copyright 2004, Information Inc., Bethesda, Maryland.

Information Highways
San Jose Mercury News
The Metropolitan Transportation Commission and Caltrans will oversee implementation of the 511 Driving Times system, which will eventually estimate travel times throughout most of California's Bay Area. Some 139 sensors will be installed along Interstate 80 and parts of Highway 101 and Interstate 880 to track speeds of vehicles equipped with FastTrack devices. Information gathered from the sensors will be sent to a government database. Drivers can call the 511 travel information line to hear the latest updates on travel conditions, but legislators can use the information to plan future road improvements. However, privacy advocates are concerned that the information could be used to track individual vehicles and issue speeding tickets. [For more information about 511 Driving Times, log on to http://www.511.org.]

Work Begins on Statewide Communication System
Associated Press
In an effort to facilitate communication between agencies throughout Indiana, law enforcement and emergency officials launched Project Hoosier SAFE–T with the goal of replacing the old radio agencies throughout Indiana, law enforcement to the State, but project field coordinator Steve Skinner says the effort's total cost after 15 years should be around $160 million. The cost of the radios will fall on the agencies that choose to join the program. It will probably take longer to implement the project in one-third of the State where radio coverage is impeded by craggy terrain. State officials add that individual sites will still be prone to technical glitches that will be rectified on a case-by-case basis. [For more information on Project Hoosier SAFE–T, log on to www.in.gov/ipts/safe-t.]

New Anti-Robbery Procedures at B of A
American Banker
Bank of America, encouraged by a pilot test in Los Angeles that reduced bank robberies by 69 percent, has announced a full rollout of new security policies and equipment at its U.S. branches. The new security procedures include armed security guards, photo surveillance equipment, bulletproof barriers, new training programs, and traps that detect weapons. The announcements come after Bank of America tested the new policies and equipment at 281 Los Angeles branches in 2002. The FBI and local law enforcement groups assisted the bank during the tests, which saw bank robberies drop from 77 between June 2001 and January 2002 to just 24 during the same time period a year later.

Super-Hero Tech
ABC News
Researchers from the U.S. Army's National Protection Center at the Soldier Systems Center developed the Law Enforcement/Corrections Tactical Uniform System (LECTUS) in order to allow officers to see in the dark, protect themselves from bullets and blows, communicate with other officers with only a whisper, see through the eyes of other team members, and enter places with nosy chemists or smoke without harm. The system, which is based on the military's Land Warrior system, uses communication technology that detects vibrations in the skull when speaking and mutes loud sounds from the environment to protect the wearer from ear damage. Although LECTUS is currently designed with nylon, spandex, and ceramic plates, researchers hope future innovations will bring about smart fabrics that will reduce the weight of the system. LECTUS already is more flexible than current protection worn by SWAT teams or prison guards. Testing of the new technology, which is still in its infancy, is underway. [For more information, log on to http://abcnews.go.com/sections/sctech/FuturesTech/future06/30604.html.]

Animation Lets Murder Victims Have Final Say
New Scientist
German researchers have developed a 3D graphics program that can help forensic experts reconstruct faces from the skeletal remains of dead people found by the police. The graphics system of Kolja Kahler and Jorg Haber of the Max Planck Institute for Computer Science in Saarbrucken, Germany, and their colleagues prove response time. The $16 million system is 90 percent federally funded; TDOT officials say that the instant feedback should let the department tell law enforcement officials about problems more quickly and improve response time. The $16 million system is to be expanded to Knoxville, Chattanooga, and Memphis, and is 90 percent federally funded; TDOT Commissioner Gerald Nicey estimates that the system will add as much as 30 percent to the road system's capacity and cost far less than widening the pavement. The camera views are to go up on the TDOT website and will be fed to local television stations, and the system will be part of Tennessee's Amber Alert for missing and abducted children. Nicely says that law enforcement agencies will be linked directly to the system. [For more information, log on to www.tdot.state.tn.us/tdotmarshart.]

Files Filling Up Prison Storage Rooms
Associated Press
Iowa's prisons want to obtain State funding to store countless paper documents collected over the years on computer compact discs (CDs). The Iowa Medical and Classification Center at Oakdale alone has documented every prisoner ever held in the State, and would require an estimated $400,000 in the first year alone to upgrade its recordkeeping. Rusty Rogerson, who serves as the center's warden, estimates it would take 5 years to complete the archiving process. Oakdale collects a criminal file, a medical file, and an inmate file for each new arrival in prison, which averages to 14 new inmates each day. The records are currently contained in a 3,000-square-foot area, but officials hope to eliminate permanent storage by destroying paper documents after their information is transferred to CD. The proposal is set to go before the legislature this January and implementation of the new system could start as soon as September 1.
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 public with criminal and juvenile justice- and drug-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.org. 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 and calendar of events databases.

Stay informed. Register at http://puborder.ncjrs.org/register to receive—

• NCJRS Catalog. A bimonthly periodical that highlights recent publications and contains a convenient online order form.
• 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.

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

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

NCJRS Contact Information at a Glance

Web: http://www.ncjrs.org
Phone: 800–851–3420 (Monday – Friday, 8:30 a.m. to 7:00 p.m. EST).
Fax: 301–519–5212 (requests for assistance).
Mail: NCJRS, P.O. Box 6000, Rockville, MD 20849–5000.

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

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

Where’s My TechBeat!

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

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 summer 2003 issue of TechBeat, published by the National Law Enforcement and Corrections Technology Center, a program of the National Institute of Justice, 800–248–2742.”

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

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

Photo Credits: Photos used in this issue of TechBeat copyright © 2003 PhotoDisc, Inc.; Corbis Images; Digital Vision; National Law Enforcement and Corrections Technology Center–Northwest; and National Corrections and Law Enforcement Training and Technology Center.

Staff: Managing Editor, Rick Neimiller; Writers, Becky Lewis, Jackie Siegel, and Stephanie Neuben; Editor, Michele Coppola; Assistant Editor/Writer, Brian Higgins; Graphic Designers, C. Denise Collins and Tina Kramer.

LOG ON TO: www.justnet.org

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

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

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

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

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.
Late one afternoon last August, the San Joaquin County (California) Sheriff’s Department received a report of a strong-arm robbery. Four men had grabbed a wallet and ripped a gold necklace from the neck of a male victim walking with a friend. Deputies John Davis and Dave Konecky arrived on the scene 17 minutes later.

During the initial interview, the victim described the suspects, including their race and approximate ages. He reported he had met one of the suspects before, but could recall only his first name. Davis entered the first name, race, and 3-year age range of the suspect into the mobile data computer (MDC) in his patrol car. Seconds later a photo, address, and phone number appeared on the screen. Davis called the victim over, who made a positive identification.

The deputies tracked the suspect to his home, where they spoke with him and a second man. Both men admitted to being at the robbery scene, but each claimed not to have taken the victim’s property. Neither would name the other two men involved. Both were taken into custody and charged with strong-arm robbery.

Because the CusInS Photo Viewer is in the startup folder on every MDC, deputies can access the program with a touch of the screen. Once the program is on screen, deputies can search any field to create candidate lists. As more particulars are entered, the search is narrowed or returns an exact hit. If the photo does not match the suspect, the suspect cannot be found, the search can proceed until a match is found or the deputy returns to the station. Because many suspects are repeat offenders, 60 percent of all suspects booked by the sheriff’s department already have a photo in the system. As more photos enter the system, Hennig expects that the positive hit rate will grow.

Accessing the CusInS Photo Viewer has been made as easy as possible. Hennig says deputies were responsible for all of the screen design and search scenarios. Every deputy trained to use the MDC can operate the photo viewer with 10 minutes or less of training. All training is done as part of normal briefings with the aid of a laptop and projector. Hands-on training is completed the first time the deputy uses the program in the car. “Our deputies have become so adept as users of this program that it is now as critical to their job as their weapons, radio, vehicle, and maybe partners,” Hennig adds. “Without this tool, many suspects would have walked for lack of a positive ID.” The MDCs are updated wirelessly each day with no degradation to radio frequency traffic or functions. It takes about 1.25 minutes of downloading to update a day’s worth of photos and associated demographics (phone numbers, addresses, etc.). If it were just adding or replacing photos, the time would be cut in half. Hennig says complaints about the system are minimal and mainly relate to the accuracy of the information—a data entry issue. Work is underway to add juvenile mug shots to CusInS as well as to expand its use to all county law enforcement agencies.

Development and deployment of the CusInS Photo Viewer was funded by a 2001 Making Officer Redeployment Effective (MORE) grant from the Office of Community Oriented Policing Services (COPS). This grant built on the earlier MDC and wireless network project, which was funded by a 1998 COPS MORE grant.

For more information on the development and implementation of the CusInS Photo Viewer, call Tom Hennig, project manager, San Joaquin Sheriff’s Department, 299-468-4423, or email hennig@co.san-joaquin.ca.us.
“There’s a lot going on, and obviously people want to be part of this,” Park says. “The vendors want to get the technology out there, and sometimes, when they give demonstrations at conferences and meetings, they don’t get to show it to the end user. This event allowed the end users to see and use it.”

Those end users owe their opportunity to see that technology to a group of area emergency medical technicians (EMTs) who began planning the first mock disaster drill early in 2001, according to NCLETTC Director Steve Morrison. That group brought NCLETTC into the process to help it obtain funding, Morrison says. After September 11, its members realized that communities need to prepare to deal with all aspects of a disaster. The group called on NCLETTC’s resources to help bring fire departments, law enforcement agencies, and hospitals into the planning process.

What started out as an EMT-only drill became Mock Disaster 2002. That initial event featured only one scenario—a chemical attack by a domestic terrorist group on spectators and a high school band at a political rally.

“It has been a unique experience to see the first-responder community coming together to work on this project,” Morrison says. “More importantly, we have seen agencies partnering and working together because of their knowledge of each others’ capabilities, training, and equipment. This is the ultimate in community team building.”

In addition to helping secure funding and bringing other agencies on board, NCLETTC, located in the former West Virginia Penitentiary in Moundsville, has the ideal facilities to host the mock disaster. When not hosting such special training events as mock disasters or the annual Mock Prison Riot, Morrison says, NCLETTC facilities are open to corrections, law enforcement, and other public safety agencies for training. Some portions of the penitentiary have been renovated into state-of-the-art classrooms, but most of the cells remain untouched and can be used for practice in cell extraction, prisoner restraint and control, hostage negotiation, and more. In addition, public safety professionals can attend scheduled classes at NCLETTC, vendors can rent space to put on demonstrations, or agencies can rent facilities for use in training exercises. NCLETTC also offers basic and advanced computer classes to the general public with more community outreach projects being planned.

For more information about the National Corrections and Law Enforcement Training and Technology Center, its programs, and facilities, call 304–843–4147, or visit the center’s website at www.nclettc.org.