National Law Enforcement and Corrections Technology Center

TECH b·e·a·t

Summer 2000

Dedicated to Reporting Developments in Technology for Law Enforcement, Corrections, and Forensic Sciences

Horse Farm Detention Center

What could the lush rolling hills of Kentucky's horse country possibly have in common with a state-of-the-art correctional facility? Not much. At least not until the court ordered the city of Lexington and surrounding Fayette County to relieve inmate overcrowding by June 2000. That was when local officials ponied up more than $70 million for a new detention center that would be located in the heart of thoroughbred horse farms.

But they are not just any old horse farms. These farms are home to some of the world's premier breeders and trainers, including such prestigious farms as Three Chimneys, home of 1997 Kentucky Derby and Preakness winner Silver Charm and 1977 Triple Crown winner Seattle Slew.

Situated in the middle of this exclusive, genteel enclave were 71 beautiful but unkempt acres. "We wanted to take this land over and utilize it as a detention site, but first we had to assure the owners of the farms along this corridor that we would incorporate the horse farm look," says Ray Sabbatine, administrator of the Lexington-Fayette Urban County Detention Center.

After 2 years of construction, the new facility opened in May 1999. It sits on scenic Old Frankfort Pike, greeting visitors and passers-by with a beautiful pond at the front of the property and triple-planked white wood fencing around the perimeter. The administration building sits atop a hill and looks remarkably like all of the other horse barns in the area. It is flanked on either side by a 7-foot-tall concrete wall with a facade that looks like a rambling stone fence. Such a pastoral scene is amazingly deceptive. For behind that wall, at the foot of the hill, about 1/2-mile away and completely invisible from the road, is one of the most technologically advanced prisons in the State.

The facility houses all levels of prisoners, "from Otis the town drunk to multiple murderers," Sabbatine says. The goal was to create small groups to make management safer and more efficient. "When you have eight dorms of eight beds each, you have a lesser apparent density of your population, simply because you've broken it down into smaller, more manageable groups."

According to Sabbatine, the prison employs the "sub-dayroom concept," a design that allows corrections officers to supervise large numbers of inmates. Sub-dayrooms in each of the facility's "pods" house eight inmates each. There are eight sub-dayrooms per pod. The sub-dayroom is typically used for passive

(See Horse Farm, page 3)

Photo courtesy CMW, Inc.

Catching the Cyber Crook

Inset photo by Aspen Systems Corp.

It's a "win-win." And the only losers . . . those intent on committing electronic crimes.

That win-win is the New York Electronic Crimes Task Force (NYECTF), a partnership between the U.S. Secret Service and a host of other public safety agencies and private corporations engaged in a fight against electronic crime.

NYECTF was formed in January 1995, according to Robert Weaver, assistant to the special agent in charge of the task force. Prior to 1995, it was a small squad of Secret Service agents primarily involved with telecommunications fraud. "But criminal abuse of technology followed the evolution of technology," Weaver says. "As technology improved and became more sophisticated, so did the criminal enterprises that were abusing it. We followed that trend."

Weaver says it had become obvious that the already successful 10-agent squad was going to require support and input from outside agencies if it was going to branch out and stay on top of technology developments. Turning the squad into a task force, he says, allowed its members to form partnerships with outside entities. Today, that membership represents 25 law enforcement/criminal justice agencies, 45 private companies, and 3 universities.

Cases typically are generated by the proactive investigation by Secret Service agents, member agencies, or nonmember departments or companies that simply need help, Weaver says. The task force has an open-door assistance policy and will help any agency that requests assistance "with no strings attached."

Each case is headed by a group supervisor or group leader. "But, we don't assign the best cases to our [Secret Service] agents," Weaver says. "Whoever brings in the case keeps the case, and we wrap the task force around them. Not all of the NYECTF's group leaders are Secret Service agents. They come from a number of outside agencies."

These "outstanding investigators," as Weaver calls them, can make command decisions and are responsible for putting a case together and for the safety of its operation. Jurisdictional problems are solved by coordinating with the U.S. Marshals Service to deputize those who are not Federal officers so they can execute Federal search and arrest warrants.

"We let what's in the best interest of the case decide how it gets worked," Weaver says. "We do a significant amount of State prosecution at the district attorney level. But if penalties are more severe under Federal statutes, we'll move to the Federal level."

(See Cyber Crook, page 2)

Image by Susan LeVan, Artville.

A History of Success

The initial U.S. Secret Service electronic crime squad and subsequent New York Electronic Crimes Task Force have had significant accomplishments and several "firsts" since beginning the investigation of electronic crimes. Robert Weaver, assistant to the special agent in charge of the task force, points to the team's 750 arrests and convictions and its $7 million in seized assets as proof of continuing success.

1993 A well-dressed, polished, impeccably credentialed and obviously professional 50-year-old former bank president convinces the manager of an upscale mall in Manchester, Connecticut, to rent space for an automated teller machine (ATM). But the machine is a fake. Over a 3-day weekend, the perpetrator and his two assistants glue shut the openings in the real ATMs, and use the fake one to collect credit card, debit card, and PIN numbers. They then empty out their victims' bank accounts and "bust out" the limit on the credit cards, netting about $120,000 in stolen goods and services. Six weeks later, the perpetrators are arrested by Secret Service and Drug Enforcement Administration agents while preparing to set up another ATM in a Coral Gables, Florida, mall. It is the end of a 10-year crime spree for the leader, a sophisticated, serious, extremely talented computer expert who writes source codes for computer programs and does demographic studies on target areas prior to installing a new ATM. It is one of the country's first cybercrime attacks on financial institutions.

1995 Secret Service agents pose as drug dealers in search of cheap telecommunications equipment after receiving a tip that it is being sold illegally and internationally on the Internet. In this, the first e-mail wiretap in the United States, they eavesdrop on a transaction. In their role as drug dealers, the agents agree to purchase a sophisticated piece of equipment that intercepts wireless messages for their narcotics operation. The device was developed and was being sold by a talented, well-educated German engineer who speaks three languages and routinely travels to Hong Kong, Taiwan, Europe, and the United States. The engineer is subsequently arrested, convicted, and sentenced to serve 51 months plus a probationary period.

1997 The president and vice president of Breaking News Network, a legitimate news agency, are arrested after Federal officers discover that they have been intercepting the voice and text messages of the New York police and fire departments' commanders. Reporters use the information to scoop their rival media outlets on breaking stories. In particular, they are credited as the first to publicize the story of the Trans World Airlines Flight 800 crash. The maximum penalty for this type of crime, however, is only 6 months' probation per charge. The defendants plead guilty to two charges—illegal interception and dissemination of the police and fire departments' messages. They both receive 12 months' probation.

1999 Federal agents arrest a man selling equipment to intercept information transmitted between police headquarters and the mobile data terminals in patrol cars, and between ambulances and hospitals. This equipment allows the user to access emergency services traffic that includes such sensitive and personal data as accident information, blood type, and physical allergies of crash victims, which can then be changed and retransmitted to the hospital. They can also intercept police transmissions, including incident information, charges, driver's license number, date of birth, criminal history, Social Security number, occupation, and home address. In one case, a Nassau County, New York, resident uses his interception equipment to learn that the local SWAT team is getting ready to execute a high-risk arrest warrant. The radio dispatcher informs all marked units to stay clear of the target area so the suspect will not be forewarned. But the buyer of the equipment immediately posts the SWAT team's plan on the Internet, where it can be read by anyone with a computer and a phone line, including the suspect and his associates.

(Cyber Crook . . . cont. from page 1)

Weaver says that NYECTF aims to stay on the leading edge of technology. But, because budgetary concerns always seem to make that difficult, the relationships with partner agencies and industry are the backbone of the team. "You need every asset at your disposal to take the wiggle room out for the bad guys," he says. "But that's easier said than done. That's why we see our relationships with the private sector and with the other agencies on the task force as our most important asset—more important than the cases themselves. Cases come and go."

Weaver says the task force keeps an eye on what it considers to be the top six infrastructure targets for electronic crime or cyberterrorism: financial institutions, telecommunications, the energy industry, transportation, the environment, and emergency services. In addition, task force members are active in the community, take a proactive investigative stance, and help educate private industry about "cyber" threats. NYECTF also cooperates with universities on an internship program that has graduates with computer-related degrees working either for private industry or for an area law enforcement agency.

The New York Electronic Crimes Task Force also has an "open-door" policy when it comes to membership. There is only one caveat: "We do not take reformed hackers and turn them into heroes. We don't need their help. We don't want their help. The only thing we'll do with hackers is debrief them and use the information they provide," Weaver says. Otherwise, prospective members need only a willingness to share information and the ability to work as a team.

Starting your own task force can be equally simple, Weaver says. The team's most important assets should include talented people, the support of each member's department or company, the ability to track technology and the current state of electronic crime, and the ability to anticipate the future. Funding is another component. For NYECTF, he says, it comes from the U.S. Secret Service and corporate donations. The rest—hardware and software included—comes from a number of outside sources. "We are very appreciative of the private sector's cooperation and support with equipment and technology resources."

One of the members of the New York Electronic Crimes Task Force is the National Law Enforcement and Corrections Technology Center (NLECTC)–Northeast, which will lend its technological assistance to the law enforcement agencies, universities, research laboratories, and private companies comprising the task force.

This partnership will allow NLECTC–Northeast to demonstrate to both public and private sectors those technologies developed for addressing electronic crime, says Fred Demma, a member of NLECTC–Northeast's technical staff. At the same time, the Northeast center will make its knowledge base available to the task force, while learning what kinds of tools investigators need to work cases involving electronic crime. This partnership also gives center personnel the opportunity to participate in the task force's educational effort about how an information system can be compromised and how the system can be protected.

"Private industry may have been reluctant to admit they have a problem," Demma says. "But if you analyze it on a global scale, private industry has had the greatest amount of economic loss."

For more information about the New York Electronic Crimes Task Force, for assistance with an electronic crime-related case, or for task force membership information, call 212–637–4650, or contact Robert Weaver, 212–637–4647. For information about NLECTC–Northeast's participation in the task force, contact Fred Demma, 315–339–6184.

Best Practices for Seizing Electronic Evidence
A joint project of the International Association of Chiefs of Police and The United States Secret Service
Best Practices for Seizing Electronic Evidence

Best Practices for Seizing Electronic Evidence is a free, 10-page, pocket-sized manual that provides a basic understanding of key technical and legal factors regarding searching and seizing electronic storage devices and media. Covered are personal computers (including tracing e-mails), electronic paging devices, facsimile machines, caller identification devices, and smart cards.

The manual was developed as a project of the International Association of Chiefs of Police Advisory Committee for Police Investigative Operations. The committee convened a working group of various law enforcement representatives, facilitated by the U.S. Secret Service, to identify common issues encountered in today's crime scene.

To order a copy of Best Practices for Seizing Electronic Evidence, please contact the International Association of Chiefs of Police, 800–THE–IACP. The publication may also be downloaded from the association's World Wide Web site at www.theiacp.org.

Photo by Aspen Systems Corp.

Coming Up

NIJ Technology Institute for Corrections

Overview

For the third year, the National Institute of Justice (NIJ) is sponsoring its annual Technology Institute for Corrections. This technology institute, tentatively scheduled for October 22–27, 2000, in Washington, D.C., is designed for corrections managers to learn about and discuss technology initiatives and issues affecting the corrections community.

Agenda

During the week-long institute, attendees will receive information and assistance about existing and developing corrections technologies and problem solving relating to technology implementation, and exchange technology lessons learned. Attendees also will participate in briefings and demonstrations at various locations in the metropolitan area, which may include the U.S. Department of Justice, the National Institute of Justice's Office of Science and Technology, the National Law Enforcement and Corrections Technology Center, and local law enforcement or corrections facilities.

Goals

- To provide participants the opportunity for continued education on technologies applicable to law enforcement and corrections.
- To provide participants the opportunity to meet and interact with other corrections professionals.
- To provide NIJ the opportunity to improve and build upon its technology development programs based upon participant experience and comments.

Registration

Attendance is limited to 25 mid-level managers from State and local corrections and community corrections agencies involved with technology and technology initiatives within their respective departments. An agency may submit one applicant for consideration. Deadline for receiving applications is September 1, 2000. All travel, lodging, and meal expenses for participants are paid for by NIJ. Call 800–248–2742, or e-mail asknlectc@nlectc.org to receive an application or additional information.

(Horse Farm . . . cont. from page 1)

recreation. A larger area within the pod is used for delivery of various types of programming (e.g., educational, religious, orientation materials, messages about events) that originate from the system's central broadcast facility. This programming is either purchased or created and edited inhouse and then broadcast to one or all of the units.

In addition, the facility incorporates videoconferencing technology. This allows judges to talk to inmates or conduct video arraignments from chambers or a courtroom. Video visitation also is available for handicapped family members who cannot walk the length of the public corridor to the inmate living areas. Telemedicine technologies are being used for mental health evaluations and will soon come online for other medical needs. A computerized card and card readers are used by correctional officers to access various areas. The cards do not require swiping. They are automatically read when an officer presents it within 18 inches of the door.

As for perimeter security, Sabbatine says it was determined in part by the environment and by community sentiment. Because the surrounding community made it clear it did not want fences topped with concertina, prison officials used 23-foot-tall exterior walls for the prison units. The result is a windowless facility that allows light to shine in from above the recreation areas and through the cell fronts, which are made of polycarbonate. Security cameras are "all over the place," Sabbatine adds, and can be remotely and individually activated and manipulated.

Even with all the special considerations that needed to be addressed, the detention center was completed in less than 2 years (average start-to-finish on a project such as this generally runs 3 to 4 years), and came in $6 million under budget. The trick, Sabbatine says, was working with the "design-build" concept.

"The design-build concept means that you have concurrent design and building. You do 30 percent of your drawings up front, get a guaranteed cost from your builder, and start construction. At the same time, you start on your second contract. We got the idea from the private sector. We went to a design-build seminar in Florida 2 years ago when we were under court order to begin construction and have it finished by June 1999. Design-build was the only way we could accomplish it."

Photos courtesy Lexington-Fayette Urban County Detention Center.

Sabbatine credits the design-build strategy not only with saving money and time, but also with allowing officials to incorporate new technologies. "We traded out tile floors so we could [have funds to] upgrade our technology," he says. "We have concrete floors, but who cares? In most cases, we negotiated the expenditure of funds based on our original budgeted amount. That's how we pulled $6 million out of the original cost."

The detention center opened with 1,200 inmates, even though it was built for 2,200. So far, there have been no complaints from the surrounding community, Sabbatine says. Prison officials involved community members in the design process from the beginning. Once the design was displayed in a public hearing and the community saw the facility's conceptual design, support was immediate. Even the former vice mayor, Teresa Isaac, was impressed with the design. "It will be the first jail in *Southern Living*," she said when the project was first shown to the city's governing council.

For more information about the Lexington-Fayette Urban County Detention Center, contact Ray Sabbatine, administrator, 606–233–0844.

From the Director, Office of Science and Technology

Law enforcement, courts, and corrections officials and officers working in the field know how crucial technology is to their day-to-day operations. In some circumstances, having the right tool can even mean the difference between life and death.

The technological revolution that has swept society as a whole in recent years has also affected the criminal justice system. Some technologies that not long ago seemed advanced—vests that can stop bullets and electronic monitoring of probationers—today seem commonplace. But the revolution continues apace, with ever more spectacular advances now being made, or in the testing stages, or on the drawing board.

As the research arm of the U.S. Department of Justice, the National Institute of Justice (NIJ) has, since its founding 30 years ago, been in the forefront in sponsoring the development, testing, and demonstration of technology to improve the justice system. The development of DNA testing standards, soft body armor, and improved fingerprint evidence collection are some of the many areas in which NIJ has played a leading role.

More recently, with strong support from the Administration and the Congress, NIJ has accelerated the pace of its efforts. Less-than-lethal technologies to minimize the use of force, computerized mapping to pinpoint and analyze crime patterns, concealed weapons detection to prevent violence, methods of stopping fleeing vehicles to apprehend suspects, and improvements in DNA laboratories to aid in evidence testing—all these capabilities, and others, are now being explored by NIJ. Their application can mean even greater transformations in law enforcement operations.

TechBeat *plays an important role as an essential link communicating the latest information about these developing technologies from the National Law Enforcement and Corrections Technology Center. By keeping law enforcement, courts, and corrections personnel current about the tools they can use, the newsletter makes a difference in controlling crime and ensuring justice.*

David G. Boyd, Ph.D.
Director
Office of Science and Technology
National Institute of Justice

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

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

All About TechBeat

***TechBeat* is the award-winning flagship publication of the National Law Enforcement and Corrections Technology Center (NLECTC) system. Our goal is to keep you up to date on technologies currently being developed by the NLECTC system, as well as other research and development efforts within the Federal Government and private industry. *TechBeat* is published four times a year. Managing Editor, Rick Neimiller; Contributing Editor/Writer, Lois Pilant.**

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

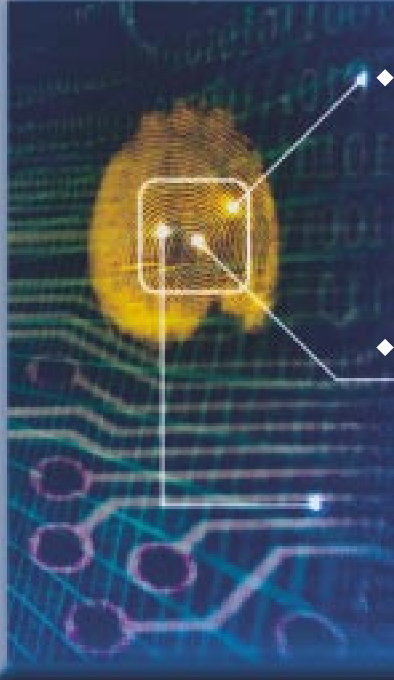
Department Subscriptions: **If your division, department, or agency has more than 25 individuals, we can drop ship as many copies as you require. All you have to do is provide us with the quantity needed, a shipping address (no post office boxes, please), and a contact name and telephone number. Your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

Article Reproduction: **Unless otherwise indicated, all articles appearing in *TechBeat* may be reproduced. We do, however, request that you include a statement of attribution, such as: "This article taken from the Fall 1999 issue of *TechBeat,* published by the National Law Enforcement and Corrections Technology Center, a program of the National Institute of Justice, 800–248–2742."**

Photos: **We are always on the lookout for good-quality photographs that depict the many aspects of the law enforcement, corrections, and forensic sciences communities and illustrate the tasks and situations they face on a daily basis. Photos should be in either color print or color slide format. Prints should preferably be 5 inches by 7 inches or larger. Duplicate prints/slides made from the originals—and not the originals themselves—should be sent, as we cannot accept responsibility for prints/slides that may be damaged or lost. Appropriate credit will be given to contributing photographers when their work is published. Please include your name and daytime telephone number when submitting any photographs. Contact Rick Neimiller, *TechBeat* managing editor, at 800–248–2742 for additional information.**

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 to rneimiller@nlectc.org.**

Target Our Site



- Information on new technologies, equipment, and other products and services available to law enforcement, corrections, and the criminal justice communities, including access to a database of more than 4,000 available products and technologies.
- Online News Summary includes article abstracts on law enforcement, corrections, and forensics technologies that have appeared in major national newspapers, magazines, and periodicals and on national and international wire services and Web sites.
- Publications from NIJ and NLECTC that you can view or download to your system.
- Interactive Topic Boards that allow you to post questions and exchange information with hundreds of professionals in their specialty areas.
- Frequently Asked Questions that offer detailed information based on thousands of calls to our information specialists.
- Calendar of Events that lists the latest upcoming meetings, seminars, and training.
- Links to other important law enforcement and corrections Web sites.

For help in establishing an Internet connection, linking to JUSTNET, or finding needed technology and product information,

call the NLECTC Information Hotline at 800–248–2742.

www.nlectc.org

A DNA Evidence Primer

National Commission on the Future of DNA Evidence

Just as today's law enforcement officer has learned to look routinely for fingerprints that could identify the perpetrator of a crime, that same officer needs to think routinely about evidence that could contain DNA.

Due to recent advancements in DNA technology, investigators with even a basic knowledge of how to identify, preserve, and collect DNA evidence properly can solve cases in ways previously unimaginable. DNA also can be the evidence that links different crime scenes to each other.

So, what do you know about DNA? Perhaps not as much as you should. But a brochure produced by the National Institute of Justice and the National Commission on the Future of DNA Evidence can help. *What Every Law Enforcement Officer Should Know About DNA Evidence,* summarized here, explains DNA and the related identification, preservation, and collection issues that every law enforcement officer should know.

DNA, or deoxyribonucleic acid, is the fundamental building block for an individual's entire genetic makeup. It is a component of virtually every cell in the human body, and a person's DNA is the same in every cell. However, each person's DNA is different from every other individual's, except for identical twins. Because of that difference, DNA collected from a crime scene can link a suspect to—or eliminate a suspect from—a crime. It can also identify a victim through comparison with DNA from relatives, even though there may be no body associated with a suspected homicide. And when DNA evidence from one crime scene is compared with evidence from another, it can be determined if the crime scenes are linked to the same perpetrator.

DNA is similar to fingerprint analysis in how matches are made. When using either DNA or a fingerprint to identify a suspect, the evidence collected from the crime scene is compared with a "known" print or sample. If the identifying features are the same, the DNA or fingerprint is determined to be a match. If, however, a feature of the DNA or fingerprint is different, there is no match.

DNA evidence can be collected from virtually anywhere and has helped solve cases in which investigators collected evidence from nontraditional sources (see "Identifying DNA Evidence" below). One murder was solved when the suspect's DNA, taken from saliva in a dental impression mold, matched the DNA swabbed from a bite mark on the victim. Numerous cases have been solved by DNA analysis of saliva on cigarette butts and postage stamps.

Every officer, from the first responding patrol officer to the experienced detective and the crime scene specialist, should be aware of important issues involved in the identification, collection, transportation, and storage of DNA evidence. Because extremely small samples of DNA can be used as evidence, greater attention to contamination issues is necessary. Evidence can be contaminated when DNA from another source gets mixed with DNA relevant to the case. This can happen when someone sneezes or coughs over the evidence or touches his or her mouth, nose, or other part of the face and then touches the area of the evidence containing the DNA.

When transporting and storing DNA evidence, keep the evidence dry and at room temperature. Once the evidence has been secured in paper bags or envelopes, it should be sealed, labeled, and transported in a way that ensures proper identification of where it was found and proper chain of custody. Never place DNA evidence in plastic bags because the moisture retained in the bags can be damaging to the DNA. Direct sunlight and hot conditions also may be harmful to DNA. Avoid keeping evidence in places that may get hot, such as a room or police car without air conditioning. For long-term storage issues, contact your local laboratory.

To avoid contamination of evidence that may contain DNA, always take the following precautions:

- Wear gloves. Change them often.
- Use disposable instruments or clean them thoroughly before and after handling each sample.
- Avoid touching the area of the evidence where you believe DNA may exist.
- Avoid talking, sneezing, scratching, and coughing over evidence.
- Avoid touching your face, nose, and mouth when collecting and packaging evidence.
- Air-dry evidence thoroughly before packaging.
- Put evidence into new paper bags or envelopes, not into plastic bags. Do not use staples.

As with fingerprints, the effective use of DNA may require the collection and analysis of "elimination samples." These samples are necessary to determine whether the evidence came from the suspect or from someone else. An officer must think ahead to the time of trial and possible defenses while still at the crime scene. For example, in the case of a residential burglary where the suspect may have drunk a glass of water at the crime scene, an officer should identify appropriate people, such as household members, for future elimination sample testing. These samples may be needed for comparison with the saliva found on the glass to determine whether the saliva is valuable evidence.

One investigative tool available to law enforcement is CODIS (COmbined DNA Index System). CODIS, an electronic database of DNA profiles that can identify suspects, is similar to the AFIS (Automated Fingerprint Identification System) database. All 50 States are in the process of implementing a DNA index of individuals convicted of certain crimes, such as rape, murder, and child abuse. Upon conviction and sample analysis, perpetrators' DNA profiles are entered into the DNA database. Just as fingerprints found at a crime scene can be run through AFIS in search of a suspect or another crime scene link, DNA profiles can be entered into CODIS. Therefore, law enforcement officers have the ability to identify possible suspects when no prior suspect existed.

To receive copies of the brochure, **What Every Law Enforcement Officer Should Know About DNA Evidence,** *contact the National Criminal Justice Reference Service at P.O. Box 6000, Rockville, MD 20849–6000; 800–851–3420 or 301–519–5500; or askncjrs@ncjrs.org*

Image by Digital Vision.

Identifying DNA Evidence

Since only a few cells can be sufficient to obtain useful DNA information to help your case, the list below identifies some common items of evidence that you may need to collect, the possible location of the DNA on the evidence, and the biological source containing the cells. Remember that just because you cannot see a stain does not mean there are not enough cells for DNA typing. Further, DNA does more than just identify the source of the sample; it can place a known individual at a crime scene, in a home, or in a room where the suspect claimed not to have been. It can refute a claim of self-defense and put a weapon in the suspect's hand. It can change a story from an alibi to one of consent. The more the criminal justice community knows how to use DNA, the more powerful a tool it becomes.

Evidence	Possible Location of DNA	Source of DNA
baseball bat or similar weapon	handle, end	sweat, skin, blood, tissue
hat, bandanna, or mask	inside	sweat, hair, dandruff
eyeglasses	nose or ear pieces, lens	sweat, skin
facial tissue, cotton swab	surface area	mucus, blood, sweat, semen, ear wax
dirty laundry	surface area	blood, sweat, semen
toothpick	tips	saliva
used cigarette	cigarette butt	saliva
stamp or envelope	licked area	saliva
tape or ligature	inside/outside surface	skin, sweat
bottle, can, or glass	sides, mouthpiece	saliva, sweat
used condom	inside/outside surface	semen, vaginal or rectal cells
blanket, pillow, sheet	surface area	sweat, hair, semen, urine, saliva
"through and through" bullet	outside surface	blood, tissue
bite mark	person's skin or clothing	saliva
fingernail, partial fingernail	scrapings	blood, sweat, tissue

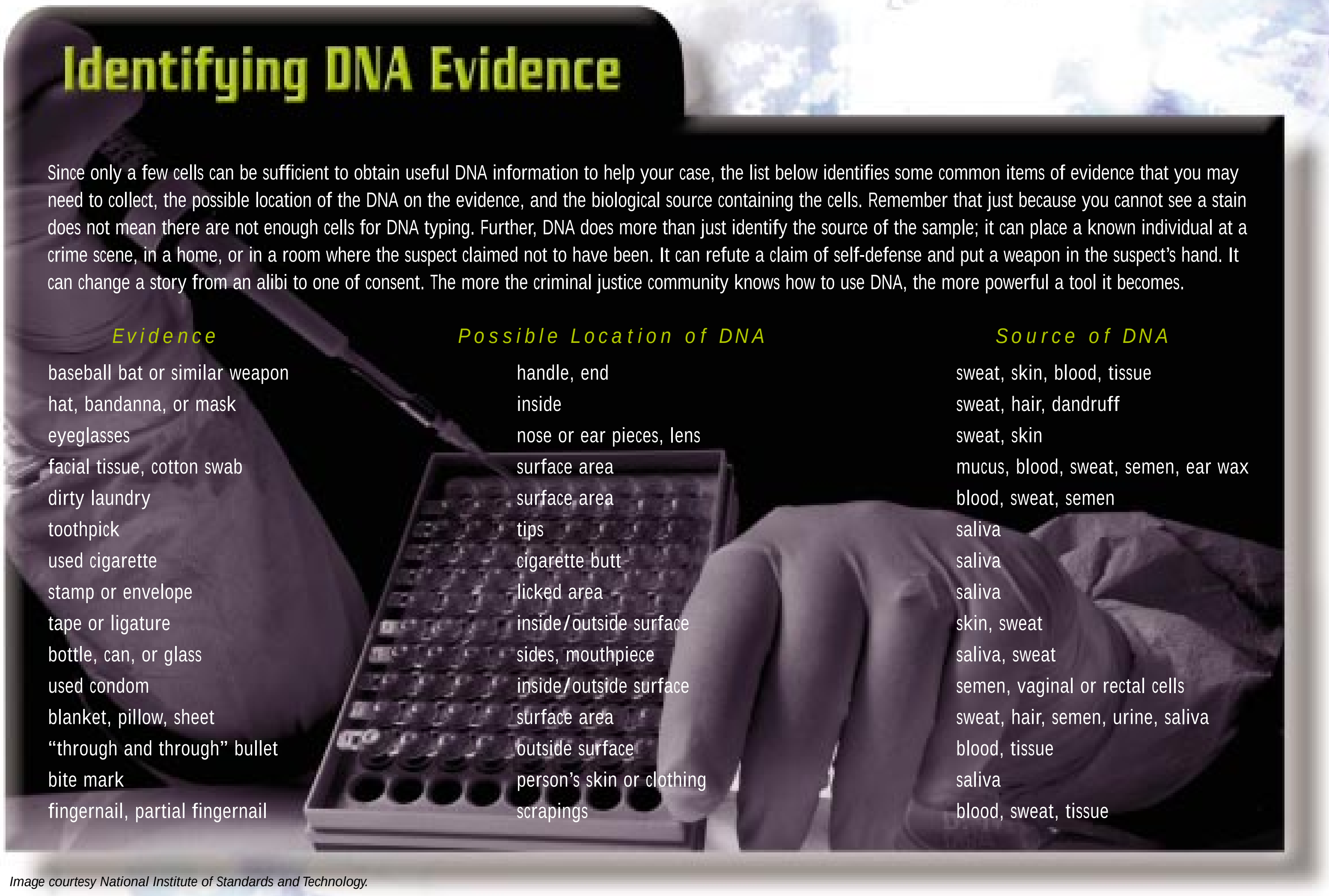


Image courtesy National Institute of Standards and Technology.

TECH SHORTS

Technology News Summary

TechShorts presents a sampling of article abstracts published weekly as part of the National Law Enforcement and Corrections Technology Center's (NLECTC's) online information service: the Law Enforcement and Corrections Technology News Summary.

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

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

Please note that providing synopses of articles on law enforcement and corrections technology or the mention of 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, and the NLECTC Law Enforcement and Corrections Technology News Summary *should be cited as the source of the information. Copyright 2000, Information, Inc., Bethesda, Maryland.*

Technology Collars 'Elvis the Hunter'

Houston Chronicle

An Elvis impersonator from Wisconsin with a long history of wildlife violations is now the first poacher to be convicted with the use of a law enforcement technology called isotope analysis. Clyde H. Masten III, 24, has a record of almost 30 previous violations of Federal hunting laws. He now is the first person convicted of poaching after isotope analysis revealed he had misled officers with a claim that his buck was from Michigan. Researchers from the University of Wisconsin helped officers catch Masten by testing his game for strontium, an element found in varying quantities in rocks, teeth, and bones depending on the geophysical environment of the specimen's place of origin. This test, which also is used to identify human remains, showed Masten's buck to be from the Portage, Wisconsin, area rather than the area of Michigan from which he said he took his game. Investigators also learned that Masten videotaped a buck in Michigan and then used a false animal tag to bolster his fraudulent claims that his catch was from Michigan. After a plea bargain, Masten faces 30 days in jail, a $2,000 fine, 1,000 hours of community service, and 5 year's probation.

Officials Eye Charging Inmates for DNA Testing

Boston Herald

Prison inmates in Massachusetts could be required to submit to DNA testing and pay a $110 fee that would go toward the establishment and maintenance of a DNA database under a current proposal. Law enforcement agencies believe a DNA database would help officers solve the most puzzling crimes, while the American Civil Liberties Union (ACLU) sees the proposal as an invasion of privacy and a tax on people who cannot afford the fee in the first place. In 1998, Superior Court Judge Isaac Borenstein sided with the civil libertarians, but in 1999, the Supreme Judicial Court in Massachusetts overturned the ruling. Violent offenders are already submitting their DNA to law enforcement agencies. The ACLU opposes DNA testing of prisoners, because law enforcement agencies could end up invading the privacy of every citizen arrested. DNA testing and DNA databases have helped officers solve crimes, but it is a high-priced program. The Plymouth County District Attorney's Office spent about $50,000 on DNA testing alone in 1998; obtaining the $110 fee from prisoners would help some law enforcement agencies pay for DNA information.

New Technology To Help Police Detect Evidence Not Visible to Naked Eye

ABC News

New video technology can reveal clues that cannot be seen by the naked eye. Catherine Dickey, a forensic scientist with the Albuquerque (New Mexico) Police Department, looked to nearby Sandia National Laboratories and engineer Colin Smithpeter to help her with a murder case. Smithpeter is designing a new video system under a National Institute of Justice grant that helps police departments find physical evidence by using high-tech optics that make bodily fluids fluoresce. It can also detect hard-to-find fingerprints. There is no need to darken the room; instead, the investigator simply scans the camera across the scene to locate evidence. This device prevents investigators from having to use chemicals and other substances that could damage DNA evidence at crime scenes.

The Lane Ranger

Atlanta Journal and Constitution

Accident reports can be invaluable when analyzed altogether, providing engineers, health officials, and law enforcement with valuable insight into road and vehicle design needs, where to concentrate medical resources, and where to patrol, respectively. Unfortunately, accident reports in Georgia and elsewhere are still largely on paper, making timely and accurate data analysis very difficult. To eradicate this problem, Georgia's State and local officials are developing software and providing police cars with laptop computers to allow officers to file accident reports directly into a database by as early as this summer, with plans to link the database to emergency medical service personnel by 2001. Health department officials can then relay that data to public works officials who maintain the roads. "With that data, you can make decisions like whether to build a concrete barrier or a more forgiving guardrail" at a given location, says Federal Highway Administration safety engineer Frank Julian.

Air Force Tests Goggles To Protect From Lasers

The State (South Carolina)

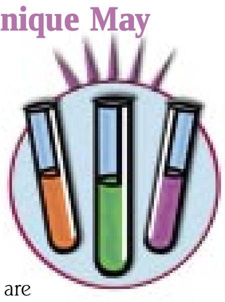
A number of U.S. Air Force crews are helping to test laser-protective goggles that could become standard issue by 2001. Air Force officials have become increasingly concerned in the last few years with the threat of lasers from enemies and their own aircraft. Some weapon systems use lasers as guides, while other lasers are designed to impair pilots' vision. Even an unintended or "friendly" reflection of a laser can damage servicemen's eyes. "I think it's quickly becoming a threat. They talk about the modern battlefield, weapons changing, technology changing. What we see as threats today, antiaircraft fire, may be upgraded the next time we go out there," says C-17 pilot Capt. Michael Carter. Law enforcement officials would also do well to don laser-protective eyewear. In a recent issue of the *Law Enforcement Bulletin*, laser expert Douglas Johnson reported how youths in the United States and Europe used lasers to temporarily blind subway drivers. Moreover, Johnson projects that low-powered lasers will increasingly be used against police.

Miami-Dade Launches Defibrillation Program

Law Enforcement Technology

In a bid to better treat sudden cardiac arrest emergencies, law enforcement officers at the Miami-Dade (Florida) Police Department have been trained to use automated external defibrillators (AEDs). Some 1,900 patrol cars, marine units, mounted units, helicopters, and bicycle patrols have been equipped with LIFEPAK 500 AEDs, which the officers are allowed to take home to ensure that the AEDs are at the community's disposal at all times. The program is believed to be the largest in the country.

Human ID Technique May Assist Police



Deseret News (Salt Lake City)

Individual Specific Antibodies, which are normally occurring antibodies in the human body, are being used in a technique called the Antibody Profile Assay to identify individuals. The technique, which was developed by the Idaho National Engineering and Environmental Laboratory (INEEL) and Miragen, a biotechnology company, could be a useful tool in law enforcement, because this type of antibody is unique to each person and the test takes only 2 hours to complete. Law enforcement is currently relying on DNA testing, which takes between 24 hours and 3 weeks to complete. According to Vicki Thompson, an INEEL researcher, the Antibody Profile technique only requires bodily fluid, not DNA material. The fluid can even be identified when mixed with dirt or animal blood and when dried on sidewalks and on cars, explains Thompson. The technique is now being tested for validity so that it can be used in a court of law, says Thompson.

Computer Forensics Teams Learn To Follow Digital Footprints

New York Times

Computer forensics is now a growing field in the criminal justice world. One of the few experts in the sector is Dr. John Leeson, an associate professor at the School of Computer Science at the University of Central Florida in Orlando. Leeson says that computers can be used not just to commit crimes, but also to store information about them. Leeson says that digital evidence can be found not only in PCs, but also in palm technology, fax machines, and cell phones. He contends that if a computer is allowed to be taken as evidence in a criminal case, it makes the job of law enforcement investigators much easier, as they can take their time and peruse the hard drive, e-mail, and World Wide Web site records to look for incriminating evidence. However, if a computer cannot be seized, it makes the investigator's job much more difficult, as digital information disappears quickly as information is overwritten. Cases in which hackers have hijacked other people's computers to launch an attack are the most difficult ones to crack, according to Leeson, since so much backtracking is involved. Because of the huge demand for computer-literate law enforcement agents, the University of Central Florida has created a graduate certificate program in computer forensics.

[Editor's note: For more information on seizing electronic evidence, ask for a copy of *Best Practices for Seizing Electronic Evidence*, a pocket-sized manual developed by the International Association of Chiefs of Police (IACP) and the U.S. Secret Service. To order a copy, contact the IACP at 800—THE—IACP, or download the manual from the association's World Wide Web site at www.theiacp.org.]

Reverse 911 Systems Can Put More Information on the Line

USA Today

Automated telephone warning systems, now in place in more than 500 law enforcement, fire, and emergency agencies, are allowing public safety personnel the same kind of quick and effective access to the public as the public has through 911. The technology integrates area maps, computers, recordings, and telephones to automatically leave specific messages on the answering machines of phones in targeted locations. The system can also be programmed to limit the messages to phones belonging to certain types of businesses, such as convenience stores, if a robbery has occurred in one of them. Costing from $15,000 to $40,000, the systems are gaining in popularity and have been used effectively to help public safety personnel warn communities about dangers or enlist the help of communities in locating missing persons.

Looking Through Walls

Man and wall photos by Corbis Images. Inset photo by Bill Fritsch,Artville.

June 1997, Pico Rivera, California—The Los Angeles County Sheriff's Department responds to a call for assistance when an armed suspect barricades himself within a business warehouse, a maze of interior office spaces, interior doors, and closets. And in the center, a pitch black open space offering a myriad of hiding places—vehicles, shelving, and debris—for him to elude capture.

The SWAT team is called when the suspect shoots multiple rounds through the walls.

The suspect is eventually discovered hiding in a small bathroom. But when attempts are made to extract the suspect, a gunfight ensues. Two deputies are wounded and the suspect is killed.

Later that same year, the National Institute of Justice (NIJ) sponsored a reenactment of this incident to demonstrate a motion detection radar technology—a two-dimensional concrete-penetrating radar device that could have been used to track the movements of the Pico Rivera suspect right through the wall. The successful demonstration of this through-the-wall technology, originally developed and built by Hughes Missiles Systems, now part of the Raytheon Systems Company, led to an NIJ grant to modify and improve this through-the-wall surveillance technology.

NIJ, through the Joint Program Steering Group (JPSG), a joint effort of the U.S. Departments of Defense and Justice in collaboration with the Air Force Research Laboratory/Information Directorate, and other organizations have sponsored research and development in technologies that would support through-the-wall surveillance for several years, according to Dr. Pete Nacci, JPSG co-chair. "Earlier efforts had shortcomings—through-the- wall systems did not provide reliable data or the data were difficult to interpret. The variability of wall construction also limited the performance of earlier systems."

The ability to "see" through walls, Nacci says, would give law enforcement and corrections operations significant tactical advantages in a number of situations. Through-the-wall surveillance can reduce the risk to officers by providing a safer way to locate hostile forces, evaluate the number of potential adversaries, and evaluate conditions for offensive operations. The data may then be used to determine the most effective use of available forces for an operation. Through-the-wall surveillance can also support search and rescue operations in hostage situations and in disaster events, such as earthquakes.

Currently, Nacci says, NIJ is funding one component of a radar-based, through-the-wall surveillance system known as MARS (Motion and Ranging Sensor). This concrete and masonry penetrating radar is an improved version of the earlier technology demonstrated at the Pico Rivera warehouse reenactment. MARS marries an enhanced two-dimensional, concrete-penetrating radar technology with three-dimensional imaging radar that can penetrate interior walls as well as map both fixed and moving objects. While the two-dimensional technology is able to detect movement, the three-dimensional imaging offers the ability to "see" depth or range.

"The MARS operator can display many different views of a potential situation on the computer screen," says Larry Frazier, technical manager and system developer for Raytheon. "MARS can display a birds-eye view as if the observer were looking down on the room, a side view that indicates the height of all the objects in the room, or a three-dimensional image that maps objects from any point in the room. There are an additional 50 modes of data display that can enhance each of the basic display modes."

Although the actual sensor technology remains essentially unchanged, MARS will be improved by better, faster computer hardware and software. Plans are to complement the custom software with commercially existing software to develop more readable displays. The sensor will also include data processing to analyze motion, displaying only the radar returns that represent likely human movement. The size, weight, and power consumption of this next generation through-the-wall surveillance system will also be reduced by improved electronic devices and by a newly designed three-dimensional imaging radar antenna, which represents a five-fold reduction in size.

In addition, the previous three-dimensional system weighed 90 pounds and was packed in three suitcases, while the two-dimensional system weighed 40 pounds and fit into one suitcase. MARS will weigh in at less than 35 pounds and fit into a briefcase. A single individual will be able to carry and deploy the equipment. Because it can be operated via battery and a radio frequency communication link, the user can also set up the sensor and then move to another location for safety or to conduct a hidden surveillance.

MARS is currently at the "breadboard" (a one-of-a-kind unit built to demonstrate capability) level of development, with one working demonstration unit in existence. NIJ is funding Raytheon to build four prototype units that will be assessed at the U.S. Air Force Research Laboratory in Rome, New York. NIJ will then evaluate these units with local law enforcement agencies to determine what changes, if any, are needed for a production system. A nationwide demonstration is planned for FY 2001.

For more information about through-the-wall surveillance systems, contact Dr. Pete Nacci, co-chair, Joint Program Steering Group, at 703–351–8821 or pnacci@darpa.mil. Or, contact David Ferris, technical manager, U.S. Air Force Research Laboratory, at 315–330–4408 or ferrisd@rl.af.mil.

Thunder Mountain

In the fall of 1999, the Thunder Mountain Evaluation Center at Fort Huachuca, Arizona, played host to a demonstration of through-the-wall surveillance systems sponsored by the Technical Support Working Group (TSWG). TSWG is an interagency organization that includes the National Institute of Justice (NIJ) and is responsible for developing counterterrorism technologies. The Thunder Mountain Evaluation Center evaluates many types of equipment and technologies for the military.

Thirty-six companies and organizations responded to an announcement of the demonstration. From this initial group, six were able to provide operational systems that could be evaluated in a neutral environment under a standardized demonstration protocol.

The general objectives of the demonstration were to identify the presence and general location of people in a space, identify the number of people in that space, and evaluate the minimum amount of movement needed for detection. The demonstration was set up to evaluate imaging through standard Sheetrock™ walls with wood interior studs, plaster walls over lathe, a 24-inch reinforced concrete wall, a tile wall, cinder block, wood walls, and multiple interior walls. Imaging into an aluminum trailer was successfully demonstrated by imaging through obstructed glass windows and through the nonmetallic floor.

Through-the-wall surveillance technology has great potential, but, according to system evaluators at the Thunder Mountain demonstration, there is room for improvement. Most of the systems demonstrated were too large for the anticipated end-users. The surveillance systems also need to employ more user-friendly displays to eliminate uncertainty and confusion. Limitations in radar physics mean that the images are markedly different from human visual images; instead, movement is represented by a series of dots.

NIJ is working with TSWG and Raytheon Systems Company to address these two issues.

Also in R&D: Radar Flashlight

Also in development in through-the-wall surveillance technology—the National Institute of Justice, through the Joint Program Steering Group, is sponsoring the Georgia Tech Research Institute (GTRI) to develop an inexpensive, handheld, low-power radar flashlight that will allow law enforcement and corrections officers to detect motion through interior walls. GTRI has designed a prototype unit that was able to detect an individual through sections of home siding and drywall, a wooden front door, and section of brick and mortar in the laboratory. An assessment of the radar flashlight is being conducted with law enforcement agencies nationwide through the National Law Enforcement and Corrections Technology Center–Southeast.

While the Raytheon Systems Company through-the-wall surveillance system is envisaged for SWAT applications, the GTRI-developed system lends itself to use by a police sector supervisor or by personnel in a corrections setting.

For more information about the radar flashlight, contact Dr. Pete Nacci, co-chair, Joint Program Steering Group, 703–351–8821 or pnacci@darpa.mil. Or, contact Bill Deck, National Law Enforcement and Corrections Technology Center–Southeast, at 800–292–4385 or bdeck@nlectc-se.org.

The ‘Center System’

Created in 1994 as a component of the National Institute of Justice’s (NIJ’s) Office of Science and Technology, the National Law Enforcement and Corrections Technology Center (NLECTC) system’s goal, like that of NIJ, is to offer support, research findings, and technological expertise to help State and local law enforcement and corrections personnel do their jobs more safely and efficiently.

NIJ’s NLECTC system consists of facilities located across the country that are colocated with an organization or agency that specializes in one or more specific areas of research and development. Although each NLECTC facility has a different technology focus, they work together to form a seamless web of support, technology development, and information.

NLECTC–National

2277 Research Boulevard • Rockville, MD 20850
Phone: 800–248–2742 • Fax: 301–519–5149 • E-mail: asknlectc@nlectc.org

The National Center, located just 30 minutes north of Washington, D.C., is the hub of the NLECTC system. It provides information and referral services to anyone with a question about law enforcement and corrections equipment or technology. Its staff manage the voluntary equipment standards and testing program that tests and verifies the performance of body armor, metallic handcuffs, shotguns, and police vehicles and tires. This office produces consumer product lists of equipment that meets a specific set of performance standards and also operates JUSTNET (Justice Technology Information Network), an Internet World Wide Web site that provides links to the entire NLECTC system and other appropriate sites, as well as assistance to those seeking information about equipment, technology, or research findings.

NLECTC–Northeast

26 Electronic Parkway • Rome, NY 13441
Phone: 888–338–0584 • Fax: 315–330–4315 • E-mail: nlectc_ne@rl.af.mil

NLECTC–Northeast is located at the Air Force Research Laboratory, Rome Research Site (formerly Rome Laboratory), on the grounds of the Griffiss Business and Technology Park. The center sponsors research and development efforts into technologies that address command, control, communications, computers, and intelligence. This center draws on the expertise of Air Force scientists and engineers in its development of technologies that can be used to detect weapons concealed on individuals, an effort that is expected to yield stationary equipment for use in buildings and handheld devices for field and patrol officers. Other areas of research and development include through-the-wall sensors, audio processing, image processing, timeline analysis, computer forensics, secure communications, and command/control.

NLECTC–Southeast

5300 International Boulevard • North Charleston, SC 29418
Phone: 800–292–4385 • Fax: 843–760–4611 • E-mail: nlectc-se@nlectc-se.org

Two of the focus areas of NLECTC–Southeast are corrections technologies and surplus property acquisition and distribution for law enforcement and corrections. The center facilitates the acquisition and redistribution of Federal surplus/excess property to State and local law enforcement and corrections agencies. The equipment must be used for law enforcement purposes only. Utilizing the JUSTNET Web site, the center educates law enforcement and corrections professionals about Federal surplus and purchasing programs. The efforts of NLECTC–Southeast have resulted in agencies receiving equipment they would not ordinarily have access to or might not have been able to afford due to budgetary constraints. This facility also studies the needs of corrections agencies. It is guided in this mission by a committee of criminal justice, law enforcement, and corrections practitioners that identifies requirements and sets priorities for research and development. NLECTC–Southeast is allied with the South Carolina Research Authority (SCRA) and the Space and Naval Warfare Systems Center (SPAWAR). NLECTC–Southeast’s other areas of focus include information management and technologies, simulation training, and designated special projects.

NLECTC–Rocky Mountain

2050 East Iliff Avenue • Denver, CO 80208
Phone: 800–416–8086 or 303–871–2522 in the Denver area • Fax: 303–871–2500 • E-mail: nlectc@du.edu

Located at the University of Denver, NLECTC–Rocky Mountain focuses on communications interoperability and the difficulties that often occur when different agencies and jurisdictions try to communicate with one another. This facility works with law enforcement agencies, private industry, and national organizations to implement projects that will identify and field test new technologies to help solve the problem of interoperability. NLECTC–Rocky Mountain also houses the Crime Mapping and Analysis Program, which provides technical assistance and training to local and State agencies in the areas of crime and intelligence analysis and geographic information systems (GIS). The Rocky Mountain facility also conducts research into ballistics and weapons technology, as well as information systems. Sandia National Laboratories has been designated as a satellite of NLECTC–Rocky Mountain. The laboratory works in partnership with NLECTC–Rocky Mountain and focuses on technology for detecting and neutralizing explosive devices.

NLECTC–West

c/o The Aerospace Corporation • 2350 East El Segundo Boulevard • El Segundo, CA 90245–4691
Phone: 888–548–1618 • Fax: 310–336–2227 • E-mail: nlectc@law-west.org

NLECTC–West is housed on the grounds of The Aerospace Corporation, a nonprofit corporation that provides technical oversight and engineering expertise to the Air Force and the U.S. Government on space technology and space security systems. NLECTC–West draws on The Aerospace Corporation’s depth of knowledge and scientific expertise to offer law enforcement and corrections the ability to analyze and enhance audio, video, and photographic evidence. In cooperation with The Aerospace Corporation, this NLECTC facility also has available an extensive array of analytic instrumentation to aid in criminal investigations, such as a scanning electron microscope, an x-ray microscope, and a mass spectrometer, all of which are used to process trace evidence. Its other areas of expertise include computer architecture, data processing, communications systems, and identifying technologies to stop fleeing vehicles.

Border Research and Technology Center (BRTC)

225 Broadway, Suite 740 • San Diego, CA 92101
Phone: 888–656–BRTC (2782) • Fax: 888–660–BRTC (2782) • E-mail: brtcchrisa@aol.com

The Border Research and Technology Center works with the Immigration and Naturalization Service, the U.S. Border Patrol, the U.S. Customs Service, the Office of National Drug Control Policy, and the U.S. Attorney for the Southern District of California to develop strategies and technologies that will facilitate control of the Southwest border. One of its most recognized accomplishments has been the implementation of SENTRI (Secured Electronic Network for Travelers’ Rapid Inspection). BRTC also works on joint ventures to identify technologies that will stop fleeing vehicles and is currently participating in a project to detect the heartbeats of people concealed in vehicles or other containers.

Office of Law Enforcement Standards (OLES)

100 Bureau Drive, Stop 8102 • Gaithersburg, MD 20899–8102
Phone: 301–975–2757 • Fax: 301–948–0978 • E-mail: oles@nist.gov

Supported by NIJ, the Office of Law Enforcement Standards applies science and technology to the needs of the criminal justice community. While its major objective is to develop minimum performance standards for equipment and technology, which NIJ promulgates as voluntary national standards, OLES also undertakes studies leading to the publication of technical reports and user guides. Its areas of research include clothing, communications systems, emergency equipment, investigative aids, protective equipment, security systems, vehicles, and weapons. It also develops measurement methods for analytical techniques and standard reference materials for forensic scientists and crime labs. Since the program began in 1971, OLES has coordinated the development of nearly 200 standards, user guides, and advisory reports. Housed at the National Institute of Standards and Technology, OLES works closely with NLECTC–National to conduct tests and to guarantee the performance and quality of equipment used by police and corrections.

Office of Law Enforcement Technology Commercialization (OLETC)

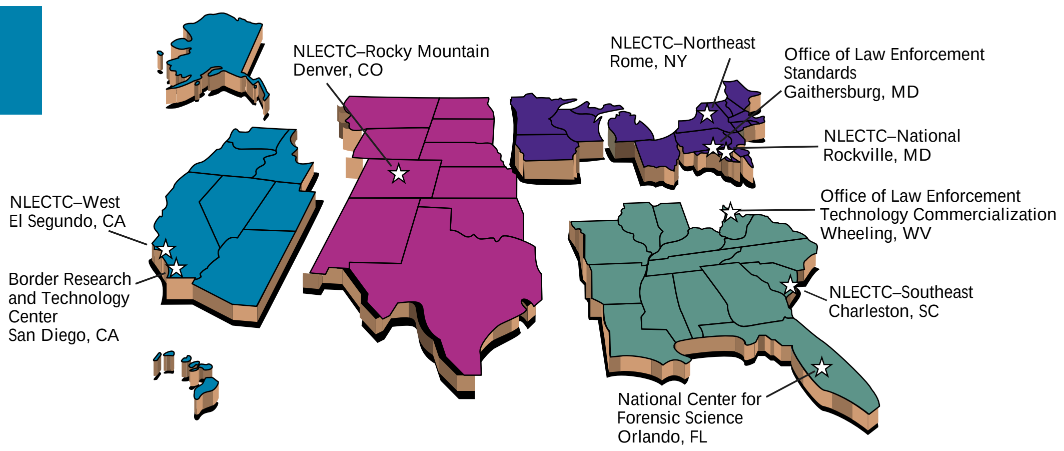
Wheeling Jesuit University • 316 Washington Avenue • Wheeling, WV 26003
Phone: 888–306–5382 • Fax: 304–243–2131 • E-mail: oletc@nttc.edu

The Office of Law Enforcement Technology Commercialization, a program of NIJ, is located at Wheeling Jesuit University. OLETC’s mission is to work with industry, manufacturers, and laboratories to facilitate the commercialization of technologies for the law enforcement and corrections marketplace. OLETC provides special services and assistance to innovators, entrepreneurs, universities, Federal and other laboratories, and U.S. manufacturers nationwide in commercializing technologies that will enhance the effectiveness of law enforcement and corrections practitioners. A national partnership is being developed to provide a continual pipeline of innovative products, concepts, and value-added services that will expedite the commercialization of new products and services needed for State and local law enforcement and corrections communities. OLETC has directly assisted in commercializing several innovative products, including the RoadSpike™, a novel vehicle-stopping device; Tiger Vision®, a special low-cost, handheld night vision device; an Explosive Ordnance Disposal Technician Training Kit; and the Counterpoint Stab and Slash Protective Vest. OLETC has identified more than 70 additional emerging technologies and concepts that are currently being evaluated for possible commercialization.

National Center for Forensic Science

University of Central Florida • P.O. Box 162367 • Orlando, FL 32816–2367
Phone: 407–823–6469 • Fax: 407–823–3162 • E-mail: natlctr@mail.ucf.edu

The newest addition to the NLECTC system, this facility is housed in the University of Central Florida and initially will focus on arson and explosives research. Its mission is to conduct fundamental research into the basic nature of fire and explosion reactions, provide the support to develop standard protocols for analyzing arson and explosion debris, promote the use of electronic media to access and exchange information about the forensic sciences, and provide educational opportunities to practicing professionals and full-time students. This new facility will draw on the experience and expertise of the university, which houses a forensic science program with an active research program, as well as the Institute of Simulation and Training, which is currently exploring ways to simulate explosive reactions to study various chemical processes.



NEW Publications

The following publications are available from the National Law Enforcement and Corrections Technology Center–National:

🖥️ 📖 ***Equipment Performance Report: 1999 Autoloading Pistols.*** This report provides a complete listing of the test data obtained during NLECTC's recent evaluation of autoloading pistols to determine their compliance with *NIJ Standard-0112.03 (Revision A)*. The report contains test results and data from 23 models of autoloading pistols, provided by eight manufacturers.

🖥️ 📖 ***Understanding Wireless Communications in Public Safety, A Guidebook to Technology, Issues, Planning, and Management.*** This guidebook was developed to help unravel the issues, terms, and options surrounding wireless communications. The publication targets managers who are responsible for funding and/or managing communications at their agencies, but who have little or no technical background in wireless technology.

🖥️ 📖 ***National Law Enforcement and Corrections Technology Center Publications Catalog 2000.*** This document provides a listing of NLECTC and other government publications of interest to law enforcement, corrections, and forensic science practitioners. Categories include communications, forensics, less-than-lethal weapons, protective equipment, and weapons and ammunition.

🖥️ 📖 ***TechBeat, Spring 2000.*** This *TechBeat* features research done on stab-resistant body armor, computer technology used to help prosecutors secure guilty pleas in the murder of a young boy, studies on the effectiveness of blunt trauma projectiles, and a database that uses records of automotive paint samples analyzed to pinpoint the manufacturer, make, model, and year of a suspect vehicle.

🖥️ 📖 ***TechBeat, Winter 2000.*** Articles discuss an innovative training program for bomb technicians; Sandia National Laboratories' "vulnerability analysis" project for prisons; and the Infotech initiative, a project that allows officers at fixed or mobile locations to enter queries and search databases in other jurisdictions.

The following publications/videos will be available soon:

🖥️ 📖 ***A Guide to Law Enforcement, Corrections, and Forensic Technology Resources Within the Office of Justice Programs.*** This first-of-its-kind resource guide delivers valuable information on law enforcement and corrections technology programs and activities of the U.S. Department of Justice's Office of Justice Programs, including available technologies; funding sources and demonstration programs; equipment standards, testing, and evaluation; current research and development initiatives; and training.

📼 ***2000 Mock Prison Riot Video.*** This videotape features technologies used to quell a mock prison riot staged by the National Institute of Justice's Office of Law Enforcement Technology Commercialization. Emerging technologies were incorporated into training scenarios to demonstrate the latest crimefighting technologies.

To obtain any of the above publications or videotapes or to receive additional copies of the* TechBeat *newsletter, write NLECTC, P.O. Box 1160, Rockville, MD 20849–1160; telephone 800–248–2742. Publications can also be downloaded from JUSTNET at www.nlectc.org.

🖥️ ***= Online*** 📖 ***= Printed*** 📼 ***= Video***

Publication images copyright © 2000 PhotoDisc, Inc., unless otherwise indicated.

Sign Up To Receive Free Reports From the National Criminal Justice Reference Service

In addition to funding the National Law Enforcement and Corrections Technology Center, NIJ supports the National Criminal Justice Reference Service (NCJRS), an international clearinghouse on crime and justice information. NCJRS staff respond to reference questions, provide referrals to other resources, distribute NIJ and other Office of Justice Programs (OJP) documents, and maintain a mailing list of more than 45,000 registered users. In addition, NCJRS sponsors the *NIJ Criminal Justice Conference Calendar* at http://www.ncjrs.org/calendar, which lists conferences and meetings of interest to the criminal justice community. If you are interested in signing up for the NCJRS mailing list, you may request a registration form using any of the following methods:

Fax-on-Demand

Dial 800–851–3420, select option 1, then option 2. The registration form is #1 on the document index. The form will be faxed to you immediately.

Fax

You may fax your request for a registration form to 410–792–4358. You will receive a form promptly in the mail.

E-mail

Send an e-mail to askncjrs@ncjrs.org and request a registration form. It will be sent to you in the mail.

Write

Send a written request to NCJRS, P.O. Box 6000, Rockville, MD 20849–6000.

Call

You may call an NCJRS information specialist and request a registration form. The number is 800–851–3420.

As a registered user, you will receive the bimonthly *NCJRS Catalog*, the *NIJ Research Review*, and selected reports based on your criminal justice interests. For more information about NIJ and NCJRS, visit their Web sites: http://www.ojp.usdoj.gov/nij and http://www.ncjrs.org.

‘Policing’ Internet Use

According to a survey by Information Week Magazine, *40 percent of employees spend at least 1 hour a day surfing the Internet without a business purpose.*

Every day, millions of Americans log onto their computers to check e-mail, catch up on the news, and research the vast amount of information to be found in cyberspace. Many criminal justice agencies now depend on the resources and information available via the Internet and allow their personnel unrestricted access. However, this access can be abused if guidelines are not in place for its proper use.

The amount of communication effected through the Internet is growing at an amazing rate. According to Michael Overly, a lawyer with a Los Angeles firm and author of *E-Policy: A Guide to How Corporations Can Deal with the Internet,* more than 1 million messages pass through the Internet every hour. With the increasing use of the Internet by law enforcement and corrections agencies, administrators now face a new problem: how to police their own employees’ use of cyberspace while on the job.

“It is especially important for public entities to manage their Internet resources properly,” Overly says. Public entities are subject to open records requests. These requests can cover such information as an employee’s incoming and outgoing e-mail messages, records of visited and “bookmarked” Internet sites, and downloaded files saved to an employee’s computer or the agency’s network.

So, how much control should a department have over Internet access by employees and how much privacy are employees entitled while they conduct business on the Internet?

Overly recommends that the best solution is to adopt a clear, concise Internet use policy so that the department can reduce the potential liability to employees and those outside the agency as well as protect confidential information and reduce the waste of the agency’s computer resources. “If employees are downloading large files and storing them on their drive,” Overly says, “it can affect the functionality of the entire system.”

When developing a policy, a few critical areas must be addressed. Overly recommends that:

- The agency educates personnel regarding privacy issues, reiterating that anything made available through the Internet can be read and viewed by other parties.
- Employees receive instruction on how they can maintain confidentiality in their Internet communications.
- The agency develops a concise statement of what an employee can and cannot do while on the Internet, including who has ownership of downloaded and stored files. “It’s important that an employee knows that all computer Internet files or documents on the hard drive belong to the agency,” Overly says.
- The agency has a statement that a violation of the policy by an employee can lead to discipline or termination. All employees of the agency should sign and date a copy of the policy.

Image by Stephanie Carter, Artville.

Overly says a good policy might begin with the following statement: “Our computer and Internet e-mail system is to be used to assist you in your job. However, you may use the system for incidental personal use, provided that your use does not impact your job function, other employees around you, or materially impact the operation of the computer system.”

Chief Walt Vanatta of Colorado’s Craig Police Department implemented a department-wide Internet use policy at the beginning of 1999. “We had some instances where we had problems with downloaded files that contained viruses or were too large for our system,” Vanatta says. “I also wanted to address personal Web sites that were created by employees. Some of them made it look like the department endorsed the site.”

Before penning his current policy, Vanatta gathered samples of similar policies from departments across the United States. He also incorporated an already existing city policy on the same issue. “Don’t recreate the wheel,” he says. “Modify various policies so that it will meet your purposes.”

Overly adds, “It takes very little to put these policies into place. In the long run, the amount of time and money saved in potential lawsuits is well worth the effort.”

For a copy of the Craig, Colorado, Police Department Internet use policy, e-mail Chief Walt Vanatta at wvanatta@ci.craig.co.us or access the document through the International Association of Chiefs of Police Web site, www.theiacp.org/.

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