Cold Case Training

Fall traditionally means back-to-school time for children and teachers across the country. This fall, another group will observe that tradition when law enforcement investigators begin to sign up for free online cold-case training offered via the Virginia Center for Policing Innovation (VCPI) Web site.

VCPI, using funding from the Office of Justice Programs’ National Institute of Justice, offered four classroom sessions of “Unsolved Cases: Cold Case Analysis for Law Enforcement and Prosecutors” in summer and fall 2009, and received approximately 700 applications from 41 states and nearly 300 agencies, nearly double the number of available seats. Fortunately, the applicants who weren’t selected as well as other investigators across the nation can take advantage of the self-paced online version, scheduled for launch in October 2009.

According to Teresa Carey, VCPI finance and marketing coordinator, both the classroom and online versions of the training use an enhanced simulation learning tool called the Virtual Case File.

The student plays the role of primary investigator and is responsible for re-examining available evidence. This evidence may include suspects, profiles, case specifics, physical evidence and lab reports. Students practice skills learned from course instruction in a simulated cold case investigation, applying investigative skills, forensic and DNA testing and more. Designed to provide a guided experience to apply tools and skills to cold case scenarios, the simulation is not won or lost as if it were an online game.

“Research demonstrates the effectiveness of practical simulations as a learning enhancement tool moving learners from simple information absorption to skill development,” Carey says.

“Every law enforcement department has unsolved cases,” says Lynda S. O’Connell, VCPI executive director. “DNA and forensic science advances have become key components to successfully solving them. By providing training in these advancements and associated investigative techniques, this program will give them the knowledge...

STEP Up to Prison Security Planning

An inmate escapes from a county jail into the community and subsequent analysis indicates that the facility’s camera system is outdated and did not help to prevent the escape. Due to the ensuing media attention, the county commissioners want to fund a major upgrade of security technology, and jail administrators need to immediately offer a plan to proceed.

Too often, that plan does not exist.

In good times or bad, correctional facilities should always have a security technology enhancement plan (STEP) ready to present, according to Gene Atherton, institutions program manager at the National Law Enforcement and Corrections Technology Center’s Weapons and Protective Systems Technologies Center of Excellence (WPSTC), hosted by the University of Denver. NLECTC is a program of the Office of Justice Programs’ National Institute of Justice.

(See Cold Case Training, page 3)

(See STEP Up to Prison Security Planning, page 2)
“A good STEP should be like a shopping list that is ready to use,” Atherton says. “In the best of all worlds, it should be one portion of an overall plan for the institutional security program. Like a shopping list, it should reflect what you want, where to get the product and the best price.”

In 2009, WPSTC helped the Security Systems section of the Texas Department of Criminal Justice Correctional Institutions Division assess security enhancement strategies. Atherton examined strategies regarding surveillance and contraband interdiction and provided valuable analysis and feedback.

“His discussion of fundamental components inherent to a security enhancement strategy was highly informative,” says Charles Bell, assistant director of security systems. “Of special interest was Gene’s insight regarding the necessity for including a process to measure the effect of applied strategies. Having the opportunity to benefit from the knowledge and experience provided by the center was significant. The analysis provided validation to much of our initiatives and added value to the security enhancement strategy product.”

Bell adds that developing a viable security enhancement strategy is essential for any correctional unit or agency, although funding these initiatives often presents a challenge for law enforcement and corrections. However, STEP preparation plays a key role in readying an agency or department to act decisively when an opportunity arises.

A good STEP should accurately reflect institutional needs, Atherton says, and must connect the proposed technology with expected performance outcomes.

“It is easy to justify technology that relates to officer safety or prevents escapes,” he says.

Decision makers presented with major funding issues require accountability. If an institution wants to strengthen perimeter technology with a detection system, administrators need to provide reliable information that past escapes have occurred through similar perimeters and that the proposed changes will make a difference, Atherton says.

“Strategies should begin with identifying the most critical need and transition incrementally toward a comprehensive package designed to achieve maximum security,” Bell says. “Constructing a global security augmentation strategy requires a series of definable objectives. From these objectives, an institution or agency develop a series of strategies that may be either independent or integrated as opportunity dictates. Collectively, they form an avenue to achieve a larger security enhancement goal.”

Atherton adds, “Technology costs and providers change constantly. However, once the format is established and support staff are made aware of the right sources of information, it should not be difficult to upgrade and adjust the plan over time.”

**A STEP has several operational segments:**

- **Perimeter security.** Includes lighting, fencing materials, electronic detection of movement on the perimeter, equipment for staff duty stations (sally ports, towers and vehicles) and electronic contraband detection.

- **Staff and inmate communication.** Involves technology related to intercoms, radios, telephones, emergency callback systems, pagers and cell phones.

- **Contraband detection.** Entails metal detectors, x-ray machines and technologies such as ion scanners.

Each plan must address an institution’s particular needs and highlight the high-priority ones. Technology specifics should include a product name, unit cost and overall summary of required funds. Suggest several different funding levels to provide options, Atherton says. The plan should also reflect short-term and long-term maintenance costs, answer how the system can be conveniently folded into an existing technology maintenance program at the facility and detail additional staff services required.

For more information on STEP in general, contact Gene Atherton at (800) 416-8086 or e-mail gene.atherton@nlectc-rm.org. For more information on Texas’ efforts, contact Charles Bell at Charles.Bell@tdcj.state.tx.us.

Each plan must address an institution’s particular needs and highlight the high-priority ones.
and skills needed to successfully investigate and resolve cold cases."

**According to VCPI materials, the course is designed to:**

- Enable nonscientists to grasp the elements of forensic biology and its implications for solving cold cases.
- Provide a practical foundation in DNA evidence identification.
- Teach about the overall knowledge, skills and best practices related to processing previously handled DNA evidence in cold cases.
- Offer guidance on identifying cases for investigation based on statute of limitations considerations and solvability factors.
- Review communication basics including verbal and nonverbal communication and impediments to effective communication.
- Provide practical case examples of successfully solved cold cases from the investigative point of view.
- Give instruction on maximizing successful prosecution of cold cases.
- Offer insight on four key elements necessary for a successful cold case homicide squad.
- Provide strategies for working with and managing the media in high-profile investigations.

“We work to anticipate training needs,” Carey says. “With the cold case training, we saw a need for the development of technical knowledge and skills to enhance efforts to successfully investigate and resolve cold cases, and we also saw a need for accessible training.”

Comments received with applications for classroom training indicated VCPI’s strategy was right on target, based on remarks such as:

- “I have been assigned to our cold case unit for DNA-related sexual assault cases since February of this year and this is the first (and most exciting) training that I have seen.”
- “Recently, my investigations unit has undertaken the responsibility of analyzing unsolved homicide cases from years past. These cases have proven to be challenging and difficult. I find myself in a position where I draw my knowledge base from experience and training related to homicide investigation geared toward a recent case. I have no training in investigating a cold case homicide. It is for this reason that your training is necessary for my own development and the investigators I supervise. . . . I value the benefit my agency gains from my attendance at this training course.”
- “My partner and I . . . are both long-time homicide detectives who have recently been assigned the task of developing a new cold case homicide unit and have been working it the past nine months. We can use all the help we can get!”

For training information, visit [http://www.vcpionline.org](http://www.vcpionline.org) or contact Teresa Carey at VCPI at (804) 644-0899, or e-mail tcarey@vcpionline.org.
From 1998 to 2007, the New York City Department of Probation used almost 50 million sheets of paper, the equivalent of nearly 625 trees, along with corresponding amounts of copier toner and printer ink, to produce reports that were sent to court. Prior to the inception of RCMS, staff keyed reports on a manual typewriter or into a word-processing template and generated seven paper copies of each report (an average 15 pages per document) to be sent to court.

Now, with RCMS on board these investigation reports are sent to court electronically and delivered into the court’s inboxes. The court clerk distributes the reports internally to the judge. These reports include information about the defendant’s current offense, history of offenses, victim statements, pedigree information and an evaluated summary made by the probation officer, who constructs the PSI on the defendant’s suitability for probation supervision and/or incarceration, and plays a key role in sentencing decisions.

“We are now in a position of saving trees, paper, copier, toner, faxes, ink, energy, all a tremendous green savings,” says Alphonzo Albright, Deputy Commissioner and chief information officer for the Office of Information Technology and Management Analysis Planning. “New York City has adopted an enormous green approach that is actively being implemented citywide, and this effort is one of the many initiatives.”

In addition to the green savings realized by the NYC Department of Probation, the advent of RCMS has also improved the department’s on-time delivery rate for reports. Albright says that when paper copies had to be delivered by hand, the department achieved only a 70-percent on-time rate, but with the onset of electronic delivery, that rate jumped to 100 percent.

Reports make up one of the many components/modules of RCMS. The first phase implemented, in 2005, is a kiosk system that allows low-risk offenders to report in electronically (using hand biometrics as identification) instead of coming to the probation office to meet with the officer assigned. This helped the probation officers to focus their time on the high-risk offenders. The use of reporting kiosks as a supervision tool automates the offender reporting process and also permits real-time information exchange. Designed with flexibility and portability, the kiosk system can be used as a standalone system or function as part of a larger case management system. Currently, 22,700 probationers report to kiosks located in department offices citywide.

“We have the reports, we have the kiosks, we have a whole suite of modules and applications that we deployed, including a data warehouse that takes in a lot of information and generates reports,” says Albright, also a member of the National Institute of Justice’s Community Corrections Technology Working Group (TWG). “Going green” is a high-priority requirement for that TWG. TWGs are associated with different NJ technology portfolios, such as corrections, and identify criminal justice technology needs within that portfolio.

Albright will be participating in the drafting of an NJ-sponsored guide on green technologies for corrections. Prior to the advent of RCMS, probation officers had to rely on unstructured database silos that provided no measure of accountability, no potential for strategic analysis and no management transparency. As the department’s needs evolved, it became obvious that the department needed an entirely new case management system.

The new system, RCMS, includes the following features:

- Real-time information exchange with various state and federal criminal justice agencies in New York City Department of Probation, the advent of RCMS has also improved the department’s on-time delivery rate for reports. Albright says that when paper copies had to be delivered by hand, the department achieved only a 70-percent on-time rate, but with the onset of electronic delivery, that rate jumped to 100 percent.

- Executive “dashboard” and management reporting capabilities. A dashboard report provides an at-a-glance perspective on the current status of a project in the context of predetermined metrics such as cost, time, requirements and/or risk.

- Data sharing that allows agencies to share critical information in emergencies and support day-to-day operations. Data sharing can take place in either real-time or through scheduled interfaces.

- New York City owns the code for RCMS, constructed by in-house information technology specialists with vendor assistance, but Albright says he is willing to work with other agencies to develop mutual sharing agreements. Possibly, he says, the source code could be made available to other jurisdictions where it could be easily modified and adapted to other agencies’ needs, and there might be mutual sharing of innovations developed by other entities. (In the context of computer science/software engineering, “reusable” means a segment of source code can be used again to add new functionalities with little or no modification; thus, it can be used by others for the original purpose or for new purposes.)

- Automation of report generation and electronic submission to various law enforcement agencies.

In addition to the green savings created by the use of RCMS, Albright offers the following tips for agencies looking to go green:

- Use your computer to eliminate paper. Write communications on up-to-date letterhead templates and design reports in your word-processing software.

- Incorporate document management that allows report development from your word-processing software.

- Print forms and memos directly from your computer instead of using preprinted forms.

- Preview database and spreadsheet printouts on your screen to ensure best use of computer paper.

- Send and receive reports and faxes from your computer instead of using printouts.

- Offer annual reports, application user manuals and major documents electronically or on disk to interested recipients.

- Consolidate forms.

- Develop Internet Web pages to provide frequently requested information.

For more information on RCMS or other New York City Department of Probation efforts to “go green,” contact Alphonzo Albright at (212) 232-0455 or email aalbrigh@probation.nyc.gov.
Researchers are going beyond traditional forensics to try and predict the physical appearance of an unidentified person whose DNA is found at a crime scene.

When DNA is taken from a crime scene, the DNA profile can be searched in the Combined DNA Index System (CODIS), which is the central nationwide database of DNA profiles, or other local DNA data banks to search for a match. In traditional uses of DNA, in the absence of a match, investigators have little or no information on a person.

Through the study of genes and pigmentation, researchers at the University of Arizona in Tucson wanted to determine, with a high degree of accuracy, hair, eye and skin color from a forensic DNA sample.

The Study

A research team led by Brilliant used 1,000 ethnically diverse student volunteers to conduct the study, paying each student $20 for their participation. Researchers measured the students’ skin tone using a skin reflectometer on the lower portion of the upper arm, where people are not likely to tan. Skin pigmentation is measured by skin reflectance. A reflectometer shines wavelengths onto the skin; what doesn’t get reflected gets absorbed. Darker skin absorbs more light.

Researchers also took hair samples from volunteers who had not dyed their hair in the past three months and determined pigment through chemical analysis. They determined eye color by comparison with an eye chart available from companies that make artificial eyes. Eye color is difficult to measure because eyes are not a uniform color.

The team then obtained DNA samples by swabbing the inside of the volunteers’ mouths along the cheeks. Information was entered into a database and the samples coded by pigmentation number and DNA number so participants’ identities were unknown. Using the DNA samples, researchers were able to predict the amount of pigment in the hair with about 76 percent accuracy. For eye color, accuracy was about 76 percent and for skin color, which is more complex, accuracy was about 50 percent.

The technology is not sophisticated enough yet to use as evidence, but has the potential to assist investigators. “This can be used as an investigative tool the same way an eyewitness account could be used as an investigative tool,” Brilliant says.

The study included collaborators from the University of Arizona Department of Ecology and Evolutionary Biology, Pennsylvania State University College of Medicine, Fujita Health University School of Health Sciences and DNA Print Genomics, Inc.

For more information, contact Murray Brilliant at (320) 626-3305, e-mail mhb@peds.arizona.edu. For a copy of the final grant report on the study, Gene Polymorphisms and Human Pigmentation, visit http://www.ncjrs.gov/pdffiles1/nij/grants/223980.pdf.

“There are instances where there are no witnesses and no matches in the DNA database,” says Murray Brilliant, Lindholm professor of genetics in the Department of Pediatrics and the Steele Children’s Research Center at the university. “I wanted to come up with a way to predict a person’s appearance, a simple DNA test to predict what a person might look like using a DNA sample.”

A goal of the study was to correlate polymorphism, or variations, in genes that are known to affect pigmentation, with variations in eye, hair and skin color. The research was supported by a grant from the Office of Justice Programs’ National Institute of Justice.
Individuals engaged in a variety of cybercrime, most notably sharing of child pornography, widely use P2P file sharing, a function best known to the general public through services similar to Napster®. Other cybercrimes that may use P2P networks include theft of copyrighted music and theft of classified government information.

Developed by ATC-NY, a subsidiary of Architecture Technology Corporation, P2P Marshal™ automatically detects use of P2P client programs, extracts configuration and log information, and lists both uploaded and downloaded shared files. It has extensive search capabilities, produces reports in several formats and runs on Microsoft® Windows®-based operating systems. P2P Marshal also provides a detailed log file of all activities it performs.

"There’s a difference between just having contraband images and disseminating them, which is obviously a more serious crime," says Frank Adelstein, technical director with ATC-NY. "An investigator needs a sense of how the suspect used the P2P tools, whether he was specifically searching for child pornography or whether he downloaded a big block of pictures and didn’t know they were included."

In order to prove intent, an investigator really needs to understand how these programs work, and every P2P program out there works a little bit differently. An investigator might have to spend a lot of time researching programs before he or she can even begin to look for information. P2P Marshal automates all of this as much as possible."

Using the tool not only saves time and thus helps eliminate backlogs, it might even help an investigator prove links between individuals and help departments expand investigations. Adelstein says that Derek Bronner, an ATC-NY employee with a law enforcement forensics background, identified a need for assistance with these issues, leading to the decision to respond to a 2006 NIJ solicitation. ATC-NY also partnered with several law enforcement agencies during the development process, obtaining their feedback and offering them the opportunity to help with beta testing.

According to Julie Baker, general manager, ATC-NY has since received numerous e-mails from officers and agencies thanking the company for developing the tool and saving investigators tremendous amounts of time. Early in 2009, P2P Marshal surpassed the 1,000-mark for registered users, while Version 1.0 of the tool was still available. Version 2.0, released in summer 2009, can be run from a USB drive and taken out into the field, whereas Version 1.0 had to be installed on a computer at a facility and run from there. This increased capability makes Version 2.0 available to field investigators and to probation and parole officers checking on compliance.

"The tool is straightforward to use, but it’s important to understand what constitutes useful evidence and what conclusions can be drawn and what questions can be answered," Adelstein says. "There are a bunch of P2P networks out there that have very different properties and it’s useful to have an understanding of how they work. As an example, someone might want to find the source of a file, and it could be that 100 different people contributed to it, so in that case, the question is meaningless."

"The tool is very easy to use. It walks an investigator through the process," says Judson Powers, a lead developer and trainer. "For those who are just getting into peer-to-peer forensics and need to get up to speed on some of the details, we offer a one-day, hands-on training class."

The class, which costs $495, offers not only training on the use of P2P Marshal, but also training on...
computer forensics related to P2P use in general.

The class covers an overview of the architecture of P2P file-sharing systems and their legitimate and illegitimate uses, forensic details commonly seen in criminal investigations, forensic analysis of client evidence and its potential pitfalls, hands-on exercises using manual analysis, and detailed instruction and hands-on exercises using P2P Marshal. At the end of the course, participants receive certification.

Powers says that ATC-NY has received comments about how easy the tool is to use from users who did not take the class, and he sees the major benefit of the class as providing understanding about P2P networks in general rather than specific information on using P2P Marshal.

“The class is really most useful for someone who isn’t doing this kind of computer forensics already,” Powers says.

Accessibility is not limited to law enforcement agencies because the tool could have civil applications, but users must provide contact information in order to register. This in turn allows ATC-NY to provide users with upgrades and patches as they become available.

To obtain Version 2.0 of P2P Marshal, visit www.P2PMarshal.com. To find out about upcoming training, phone (607) 257-1975 or e-mail training@p2pmarshal.com. For more information, contact Frank Adelstein, technical director, ATC-NY, at (607) 257-1975 or e-mail fadelstein@atc-nycorp.com.

Wikipedia provides the following definition of a peer-to-peer (P2P) computer network:

“This type of network] uses diverse connectivity between participants in a network and the cumulative bandwidth of network participants rather than conventional centralized resources where a relatively low number of servers provide the core value to a service or application. P2P networks are typically used for connecting nodes via largely ad hoc connections. Such networks are useful for many purposes. Sharing content files containing audio, video, data or anything in digital format is very common, and real-time data, such as telephony traffic, is also passed using P2P technology. A pure P2P network does not have the notion of clients or servers, but only equal peer nodes that simultaneously function as both “clients” and “servers” to the other nodes on the network. This model of network arrangement differs from the client server model where communication is usually to and from a central server.
The U.S. Department of Homeland Security’s TechSolutions program seeks to identify mission capability gaps in the first responder community and accelerate delivery of emerging technologies. The program allows responders to identify problems with existing technology or lack of technology through its Web site, http://www.techsolutions.dhs.gov.

Established in 2007 as part of the DHS First Responder Technologies (R-Tech) program within the Science and Technology Directorate, TechSolutions is open to all first responders, including fire, EMS and law enforcement. The goal of the program is to develop prototype technologies within 12 to 15 months that meet at least 80 percent of operational requirements. DHS provides up to $1 million per project, partnering with national laboratories, universities and the private sector on development.

“Our goal in TechSolutions is to provide an 80 percent or better solution to the high priority capability gaps we receive, keeping in mind that the solution must be affordable and allow first responders to do their job more efficiently and effectively,” says Greg Price, director of the TechSolutions program.

Each TechSolutions submission is vetted through subject matter experts to ensure it is a valid capability gap. If a solution is deemed feasible, DHS will work with the submitting first responder from start to finish to prototype the technology.

Capability gaps can be submitted by active or retired first responders. They can track the progress of their submission through the Web site and view the status of other projects. Since its inception, TechSolutions has received approximately 364 submissions.

TechSolutions has completed three projects: the FireGround Compass to help firefighters reorient themselves in smoky conditions, an ocular scanner capable of detecting nerve agents and toxic gases, and a handheld biometric system piloted in the Mona Pass to provide timely identification of interdicted immigrants intercepted by the Coast Guard. The Pass lies between the Dominican Republic and Puerto Rico.

“If we can take a potential life-saving concept like the FireGround Compass and work with submitters like Steve Nash of the Solon, Ohio Fire Department to turn vision into reality, we feel like we’ve done our job,” Price says.

Projects that TechSolutions is currently funding include a digital multi-band radio; an advanced personal protection system; a data fusion demonstration; a vehicle-mounted chemical detector system; and the eradication of arundo donax (carrizo cane), a quick spreading, tough to control, tall, dense weed that can provide cover to illegal aliens trying to slip across the Mexican border into the United States. According to DHS, the plant is a major impediment, in particular, to DHS-led operations between Laredo and Del Rio, Texas, overrunning border access roads, reducing visibility and hiding illegal activities.

Two additional TechSolutions projects that have generated interest are the Cylinder Array, a more compact, lighter weight self-contained breathing apparatus for firefighters, and the Dazzler, a handheld, LED-based law enforcement device that helps to neutralize aggressors with temporary, safe flash blindness effects, psychological discomfort and disorientation.

“How often do you get the chance to be part of a team developing game-changing technology?” Price says. “Take the Cylinder Array for example. This technology, when released, will dramatically reduce the weight and profile of existing self-contained breathing apparatus cylinders in use today. It will be the biggest change to the cylinder in more than 25 years.”

The R-Tech program was created in response to a congressional mandate to provide a technology clearinghouse for first responders. In addition to TechSolutions, the program includes an informative Web site, http://www.firstresponder.gov, and a monthly newsletter that features federally funded technologies being developed and tested to support the first responder community.

For more information, visit http://www.techsolutions.dhs.gov or http://www.firstresponder.gov.
On the Road to TECHNOLOGY

TechBeat is the award winning news magazine of the National Law Enforcement and Corrections Technology Center (NLECTC) system. Our goal is to keep you up to date with current and developing technologies for the public safety community, as well as other research and development efforts within the federal government and private industry. TechBeat is published four times a year.

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

Domestic Department Subscriptions: If your division, department or agency has more than 20 individuals, we can drop ship as many copies as you require. All you have to do is provide us with the quantity needed, a shipping address (no Post Office boxes, please) and a contact name and telephone number. Your only obligation is to disseminate them once they arrive. If you require fewer than 20 copies, please provide us with the names and addresses of individuals who are to receive the news magazine and we will send copies directly to them. Contact (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 Fall 2009 issue of TechBeat, published by the National Law Enforcement and Corrections Technology Center, a program of the Office of Justice Programs’ National Institute of Justice, (800) 248-2742.”

Awards: TechBeat has received numerous awards, including the 1998 Best of Category, Excellence in Printing Award from the Printing & Graphic Communications Association; the first-place 1998 Blue Pencil Award for Most Improved Periodical from the National Association of Government Communicators; the 1999 Silver Inkwell Award of Merit from the International Association of Business Communicators; the APEX 2001 Award of Excellence for Magazines and Newspapers—Print; and a 2009 Award of Excellence, External Magazine, from the National Association of Government Communicators.

Photo Credits: Photos used in this issue of TechBeat include copyright © 2009 Shutterstock; Arresting Images; Getty Images; Stock and Corbis.

Staff: Interim Managing Editor, Lance Miller; Editor, Michele Coppola; Lead Writer, Becky Lewis; Graphic Designers, Tina Kramer and John Graziano.
“Snapshot” of Southwest Border Communications Interoperability

BRTC-Western Operations and BRTC-Austin

Earlier this year, the Border Research and Technology Center-Western Operations requested the Interoperability Communications Technical Assistance Program (ICTAP) to use its Communication Assets Mapping (CASAM) Tool to provide a “snapshot” of state communications interoperability along the Southwest border. Using COFEE, the company can preserve valuable information that might be lost if an officer had shut down the computer and moved it to a lab. “We’ve changed our way of thinking recently,” says Jim Riccardi, principal electronic crime specialist at the laboratory, which is funded by NIJ. “We were taught, and have taught investigators, to pull the plug on live systems. However, with the advances in tools and research, we are now able to capture information that would otherwise be lost by pulling the plug. We now use a two-pronged approach for live systems. If it’s on, leave it on and use COFEE or a comparable tool, then pull the plug and perform the post-mortem data gathering and analysis.”

In testing, COFEE properly executed 146 of the 147 utilities. The integration of these utilities did not result in unforeseen errors or alter the output generated by executing them in an independent manner, Riccardi says. Staff also discussed their testing results with one of the utility’s principal developers; the results were reviewed and found to be accurate. Although Microsoft® has not publicly named any specific tools included in its product, the company has said that all are publicly available. Ricci Ieong and Anthony Fung, at that time members of the High Tech Crime Investigators Association’s (HTCIA) Asia South Pacific Chapter, developed COFEE in 2006. Fung, a former law enforcement officer, moved on to work for Microsoft’s Internet Safety Enforcement team in Hong Kong.

For more information or to obtain a copy of the functional analysis report, contact Jim Riccardi at (315) 838-7609 or e-mail jim@cybersciencelab.com.

Communications Benefits From Collaborative Support

Communications Technologies CoE

A partnership between the NLECTC Communications Technologies CoE and Automated Frequency Coordination Inc. (AFCo), a subsidiary of the Association of Public-Safety Communications Officials (APCO), will continue to provide ongoing technical support and consultative services to the Computer Assisted Pre-Coordination Resource and Database System (CAPRAD), in addition to administrative support to the 700 and 800 MHz Regional Planning Committees (RPCs). The latter effort is conducted through a partnership with the National Regional Planning Council (NRPC), a collaborative network of the 700 and 800 MHz RPCs. RPCs are staffed by volunteer personnel from state and local public safety agencies who often donate their time and services. CAPRAD provides a nationwide database where public safety professionals can coordinate the use of, and application for, frequencies in the limited space available in the 700 MHz band. High demand dictates that cooperative coordination is vital. CAPRAD includes spectrum reallocation by region, interactive and coordinated application for frequencies (using Federal Communications Commission Form 601) and an administrative/reporting function.

For more information, contact Carrie Supko, deputy director of the NLECTC Communications Technologies CoE at (267) 415-4760 or e-mail csupko@com-techcoe.org.

Forensic Information Data Exchange Project

Forensic Technologies CoE

A new tool is at hand to expedite sharing of forensic case information between law enforcement agencies, crime laboratories and the courts. The Forensic Information Data Exchange (FIDEX) project has created a two information data exchange packages to facilitate data submission and disposition reporting related to forensic casework. NIJ developed FIDEX through its Forensic Technologies CoE, which is hosted by the National Forensic Science Technology Center. Although many laboratories have laboratory information management systems, police departments and other agencies often use handwritten forms or send crime labs and other hard copy means to exchange data on examination results and case disposition.

FIDEX provides an electronic Web-based platform for law enforcement agencies to submit examination requests and allows crime labs to more efficiently handle case management. FIDEX is based on the National Information Exchange Model (NiEM). Pilot projects to evaluate FIDEX in a working environment are underway in the Arizona Department of Public Safety and Phoenix Police Department crime labs.

For more information, contact Robin Jones of NIJ at (202) 353-2436 or e-mail robin.w.jones@doj.gov.

New York Interoperability Consortium Follows “Best Practices”

Communications Technologies CoE and NLECTC-Northeast

New York’s Onondaga, Oswego, Madison, Cayuga and Cortland counties have banded together to create a consortium that will plan and implement interoperable public safety communications in support of fire, police and emergency medical services in the region. This consortium has followed best practices (as defined in the June 2008 NIJ In-Short Effective Public Communications Systems Require New “Governance”) in creating multi-county agreements and establishing governance prior to the implementation of any technical solutions. The NLECTC Communications Technologies CoE is observing the progress of the individual counties as they implement their own public safety voice radio systems as well as the progress of the larger consortium efforts to support interoperable communications.

Onondaga County and Madison County have made initial progress on countywide interoperable systems that will operate in the 450 MHz spectrum and will eventually share a master switch that will allow cross-county communication as necessary. Onondaga County hopes to have an operating system in place by 2009, and Madison County plans to have its system implemented in 2010. “You need agreed-upon governance and agreed-upon protocol as to when interoperability is appropriate,” says John Baloni, commissioner of the Onondaga County Department of Communications. “The biggest thing that we’ve learned is when you sit at the table and start discussing communications issues, we all find we have the same problems and the same issues. As you develop relationships with each other, that’s where the actual ability to work together comes in. You recognize that you’re all professionals dealing with the same issues. If you can get the right people to sit around a table, they find that working together toward a common solution will save time, money and energy.”

Paul Hartnett, 911 Center Director for Madison County, credits NLECTC with providing them with valuable assistance since the turn of the century that enabled them to keep their previous radio system going longer than expected and with helping with recommendations for the planned upgrade.

“The NLECTC system has been a great partner for us since 2000,” Hartnett says. “They’ve helped me with every technology issue we’ve had. They are a great resource that more counties should take advantage of.”

For more information on this consortium and the assistance being provided through the NLECTC system, contact Pete Small of the NLECTC Communications Technologies CoE at (267) 415-4770 or e-mail pete.sm@comtechcoe.org.
The National Law Enforcement and Corrections Technology Center (NLECTC) system supports the National Institute of Justice (NIJ) mission of providing objective, independent, evidence-based knowledge and tools to enhance the administration of justice and public safety. Offering free assistance to law enforcement, corrections, courts and other criminal justice agencies as well as crime laboratories—large or small, rural or urban and along U.S. borders—in the implementation of current and emerging technologies, the NLECTC system is an integrated network of criminal justice technology outreach, demonstration, testing and evaluation centers and Centers of Excellence.

The NLECTC system has been reorganized to make it more sustainable, efficient and effective in providing services to the criminal justice community.

Established in 1994 by the Office of Justice Programs’ NIJ as part of its research, development, testing and evaluation initiatives, the NLECTC system serves as an “honest broker” resource for technology information and assistance and helps introduce technologies into practice within the criminal justice community. The mission of NLECTC is to support NIJ’s research and development activities, support the transfer and implementation of technology into practice, assist in the development and dissemination of guidelines and technology standards, and provide technology assistance, information and support.

The NLECTC system seamlessly delivers its expertise to the nation’s 19,000-plus police agencies; 50 state correctional systems; thousands of prisons, jails, and probation and parole departments; courts; and crime laboratories in a number of technology areas. These technology areas are supported by technology partners who provide the leveraging of unique science and engineering expertise. In addition, technology working groups and a national advisory council provide guidance relating to the technology needs and operational requirements of the public safety community for NIJ’s various technology focus areas and help to ensure that NIJ’s activities focus on the real-world needs of public safety agencies.

Contact NLECTC for:

Technology Information
NLECTC disseminates information to the criminal justice community at no cost through educational bulletins, equipment performance reports, guides, consumer product lists, product information databases, news summaries, meeting/conference reports, videotapes and CD-ROMs. Most publications are available in electronic form through the Justice Technology Information Network (JUSTNET) at www.justnet.org. Hard copies of all publications can be ordered through NLECTC’s toll-free number, (800) 248-2742, or via e-mail at asknlectc@nlectc.org.

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 serves 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 Standards and Testing
We oversee the development of performance standards and a standards-based testing program in which equipment such as ballistic- and stab-resistant body armor, double-locking metallic handcuffs and semiautomatic pistols is tested. 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.

Technology Demonstrations and Capacity Building
We introduce and demonstrate new and emerging technologies through special events, conferences, and practical demonstrations such as the Mock Prison Riot and an annual public safety technology conference. We also provide hands-on training assistance for the latest technologies through workshops and software programs dealing with crime mapping, community corrections and critical incident management. In addition, on a limited basis, NLECTC facilitates deployment of new technologies to agencies for operational testing and evaluation.
The Office of Justice Programs’ National Institute of Justice (NIJ) is developing a standard for bomb suits worn by U.S. public safety bomb technicians. This will be the first such standard.

NIJ is developing NIJ Bomb Suit Standard for Public Safety. NIJ Standard 0117.00 at the request of the National Bomb Squad Commanders Advisory Board (NBSCAB). This standard is being developed based on research done by the U.S. Army Natick Soldier Research, Development, and Engineering Center. An expert panel of bomb technicians, other explosives community stakeholders and scientists used Natick’s research as a foundation to establish the standard.

There are approximately 470 accredited bomb squads in the U.S., and each bomb squad is required to have at least two bomb suits. These bomb suits need to provide protection while at the same time allow for user mobility and dexterity. Establishment of a bomb suit standard with standardized test methods and performance requirements ensures that bomb suits provide an established level of protection balanced with functionality.

“The bomb suit is the most critical piece of equipment a bomb technician utilizes,”Sharkey says. “A standard for the bomb suit reassures that the protection and mobility of the bomb suit is acceptable to the bomb technician and the bomb squad community. This is critical in the success of their mission.”

Optics and ergonomics capability are tested through donning and doffing, field of view and mobility tests. The standard also includes fragmentation, flame, impact and blast overpressure protection. Minimum blast pressure protection requirements are addressed through a bomb suit integrity test to determine if the suit remains intact during an explosion. Blast overpressure will be fully addressed in a subsequent version of the standard once additional research provides NIJ with a better understanding of the threats posed by blast overpressure. Also, the standard does not address chemical, biological, radiological and nuclear (CBRN) protection, which may be addressed in the future when additional research is done.

“NBSCAB supports the development of credible standards for bomb suits against each of the hazards posed by IEDs,” Hansen says. “The recent development of ergonomics, fragmentation, impact, flame and optics standards has been very important. The bomb squad community also looks forward to the development of additional standards dealing with blast overpressure, cooling suits and CBRN protection that is integrated into bomb suits.”

“With more terrorism events possible, there may be more situations when bomb technicians have to respond,” says Casandra Robinson, an NIJ visiting scientist from the Department of Energy Savannah River National Laboratory who facilitated development of the standard. “We want to make sure their equipment protects them.”

Separate documents will cover certification requirements (NIJ Bomb Suit Certification Program Requirements for NIJ Standard 0117.00) and guidance on selection and application of bomb suits (NIJ Selection and Application Guide to Bomb Suits). Manufacturer compliance with the standard, as with all NIJ standards, is voluntary.

To view a copy of the standard, certification document or selection and application guide once they are published, visit http://www.justnet.org/ctp.