NATIONAL LAW ENFORCEMENT AND CORRECTIONS TECHNOLOGY CENTER
A program of the National Institute of Justice

From Winter 2005 *TechBeat*

TECH b•e•a•t

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

Getting a 'TIP,' Making a 'Linc'

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

About iLincs

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

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

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

The instant access to information and photos that iLincs provides not only allows officers to respond to

A Common Definition

As of late fall 2004, more than 50 justice information-sharing projects, including AMBER Alert, iLincs, and ITIP, employ the Global Justice eXtensible Markup Language (XML) Data Model, better known as GJXDM, to facilitate sharing their information with other law enforcement, courts, corrections, and public safety organizations.

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

GJXDM 3.0, released in January 2004, allows disparate computer systems and networks to exchange data more

Continued on page 2

crises more quickly and efficiently—it also helps them perform their everyday duties better by allowing quicker identification of suspects and fugitives. It can even alert them to the possible dangers of a confrontation that may result from a routine traffic stop.

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

Singleton envisioned automating the process. "Imagine stopping a vehicle, doing a license plate search, and getting a full report immediately with photos and prints. Or creating a field investigative card, attaching fingerprints, and sharing it electronically. Or snapping a photo of a missing child, putting in an alert, and broadcasting it immediately from the cruiser."

In 2001, Armada began to make Singleton's vision a reality. With help from the Office of Law Enforcement Technology Commercialization (OLETC), part of the NLECTC system, the company implemented a pilot project with the Powell (Ohio) Police Department, near Armada's headquarters, in 2002.

"The idea is to reduce the amount of time an officer spends reporting or searching for information," Singleton says, "so more time can be spent policing. In my research, about 80 percent of the cost of running a department is personnel. Any time you can save officer time, you're gaining more time on the street and saving money."

"Singleton's heart is in making the operations side of law enforcement easier and more effective," says OLETC Project Manager Tom McLaughlin. "His business plan focused on small departments, and because he knew their budgets were the bottom of the barrel, he developed deals with hardware providers who agreed not to require payment upfront when cruiser PCs were purchased. If they would agree to a low monthly service fee that the law enforcement agencies could fit into their budgets, the providers would get long-term commitments from the agencies." Armada provides training and system updates at no charge.

McLaughlin first arranged for Armada to present its concept to several West Virginia law enforcement agencies. "Although they were interested in Armada's ideas," McLaughlin says, "they were reluctant to experiment with an untried technology, so I suggested that Armada run a proof-of-concept pilot." OLETC contacted Chief Gary Vest of the Powell Police Department, and in 2002, Armada installed the beta version of iLincs at the department. During the pilot project, the company refined the system based on officer suggestions and feedback.

A Common Definition (continued)

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

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

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

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

Due to the success of that project, the Ohio Office of Criminal Justice designated U.S. Department of Justice grant funds to allow six Ohio law enforcement agencies—Powell, Dublin, Upper Arlington, Westerville, Worthington, and Grandview Heights—to participate in a 2-year consortium project that started in 2003. (Several additional agencies have since used general revenue funds to join this information-sharing consortium. In addition, as a result of the success of this consortium, OLETC is currently establishing another similar information-sharing consortium with law enforcement agencies in Ohio, West Virginia, and Pennsylvania.)

As more agencies join the project, OLETC continues to provide Armada with technical assistance. "OLETC's mission is to commercialize new technologies, and there are many technologies we didn't know about that we may be able to incorporate into what we're doing," Singleton says. McLaughlin has provided contacts and introduced Armada to several additional potential technology partners, including partners that provide geographic mapping and fingerprint reader capabilities.

The Ohio State University (OSU) Police Department, one of the newer consortium partners, also is providing

development assistance. Thanks to input from the OSU police, Armada is now working on a version of iLincs for cell phone and PDA use. "An officer could search iLincs, pull up mug shots, and identify someone, using a cell phone that only costs $99," Singleton says. "OSU wants to help the campus police who are not in a vehicle but walking a beat; eventually they'd like to add student photos to verify who's supposed to be on campus. It is tremendous public relations from the police's perspective not to kick a legitimate student out of the library who simply forgot to bring an ID. Early indications are that it will be extremely beneficial to the officers."

For more information about iLincs, contact Tom McLaughlin at the Office of Law Enforcement Technology Commercialization, 888–306–5382, or tmclaugh@oletc.org.

About ITIP

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

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

ITIP enables line officers to access information about a suspect's involvement in other crimes, not only as a suspect but also as a witness or victim, according to Chris Helms, Technology Specialist Officer for the Mount Pleasant Police Department. "ITIP brings back all the cases where the suspect has been involved and provides not only suspect information, but situations where the person of interest might have been a witness or bystander or have been reporting a crime. Information on other contacts is particularly valuable for our narcotics officers."

Karen Cordray, Sergeant in Charge of Crime Analysis for the North Charleston Police Department, which serves a population of 82,000 with 177 sworn officers, agrees that ITIP's access to information on known associates is a valuable investigative tool. "We're able to do a link analysis, find the associates' names, then run the associates down. You're looking for a frequent running mate or [someone] who the person may have had disagreements with in the past."

"Bystanders will typically give you the whole world," Helms says, "because at the moment they're not in trouble. If officers can't locate a suspect, they run down the leads of the bystanders and witnesses and sooner or later, when you shake the trees, ITIP turns up your suspect." In one investigation, Mount Pleasant officers used ITIP to round up individuals known as Batman, Poopsie, and The Joker who were involved in a car-to-car shootout. Batman was identified and his address determined through ITIP. Batman identified a female bystander, whose name was in ITIP, and who subsequently identified others involved in the incident.

ITIP catches suspects who would not be detained without access to data in other jurisdictions. "Our dispatchers use it for the deputies on traffic stops and for other calls … they end up arresting people who would slip through the cracks because no warrants are entered in NCIC [the National Crime Information Center]," says Linda Driggers, Dorchester County's Training and Certification Assistant. "When our detention center does a records check, they run the name through ITIP looking for active warrants, and we often end up holding prisoners for other agencies."

But it's not just the information itself that these agencies value. "In a lot of cases where our officers use ITIP, it's not the actual solving of a crime, but how much time it saves in an investigation," says Tom Pham, Director of Research, Information Technology Division, for the 500-officer Charleston Police Department. "It has reduced manpower needs in an investigation. Before, we would have to send an officer to another jurisdiction to search their database or call them and ask them to use their manpower to provide the answers for us."

Early in their collaboration, ITIP member agencies sought technical assistance from NIJ's NLECTC–Southeast, located in North Charleston, to help develop a regional information system. NLECTC–Southeast helped develop architectural concepts and operational requirements for the network. The Southeast Center works in partnership with the U.S. Department of Defense, represented by the Space and Naval Warfare Systems Center–Charleston; the U.S. Department of Energy, represented by the Oak Ridge National Laboratory and the Savannah River Technology Center; the South Carolina Research

Authority (SCRA); and educational institutions, including the Georgia Tech Research Center.

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

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

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

According to Knight, the strength of ITIP has been the joint ownership of the executive committee. This ownership is critical, he says, because the executive committee needs the authority as a group to make decisions, manage the system for the benefit of all, and avoid power struggles and potential turf issues. Each agency in an information-sharing system should be an equal voting partner. For ITIP, this means that the chief executive officer of each member agency is on the executive committee. This committee oversees management of the ITIP system, adopts policies and procedures, and exercises final authority over all aspects of the system. The committee exercises its authority by majority vote, with each agency having one vote.

A working group regularly reviews ITIP services, Knight says, to inform the executive committee about technical and operational issues and guide the system's day-to-day operation. "The working group has discussed everything from what we want it to do for us to how we want the screens that return information to look," says Lt. John Plitsch of the Berkeley County Sheriff's Department, which has approximately 100 officers and serves an area about the size of Rhode Island.

"Nearly all of the working group members have been on the street in uniform wishing we had access to this data," Helms says, "so we know what the line-level officer wants."

According to Knight, the ITIP system connects each member agency's records management system (RMS) via redundant, high-speed, dedicated lines that end at SCRA, the site of a central data warehouse to which all agencies have access. Routers are installed at each agency and at SCRA to coordinate information transmission. Firewalls, user codes, and passwords ensure data and user security.

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

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

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

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

she says her agency now exchanges e-mails with others regarding significant incidents.

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

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

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

For more information about the Low Country Information Technology Improvement Project, contact Coleman Knight, 800–292–4385 or nlectc-se@nlectc-se.org.

For more information on managing technology projects, see* A Guide for Applying Information Technology in Law Enforcement *at www.justnet.org/pdffiles/infotechguide.pdf or* Law Enforcement Tech Guide: How to Plan, Purchase and Manage Technology (Successfully!), A Guide for Executives, Managers and Technologists *at www.cops.usdoj.gov/default.asp?Item=512.

This article was reprinted from the Winter 2005 edition of *TechBeat,* the award-winning quarterly newsmagazine of the National Law Enforcement and Corrections Technology Center system, a program of the National Institute of Justice under Cooperative Agreement #96–MU–MU–K011, awarded by the U.S. Department of Justice.