



Integration News

CRIMINAL JUSTICE DATA INTEGRATION

March/April 2004

vol. 1, no. 2

In this Issue

Florida's Integrated Criminal History System

by Pearl Adams Terrell . . . 1

MATRIX Loses Two States 7

Case Study: Using XML for Alaska Criminal Justice Data Exchange

by Steve Horneman and
Nancy LaPlaca 8

A Report to Congress on the Information Sharing Needs & Requirements of the Office of the Sheriff

by Dr. Lee Colwell 12

Integrated Databanks Cause Concern for Foreign Visitors 19

Private Sector Responds to WA Call for Education by Brian LeDuc 20

Maryland Counties Create Integrated Network . . . 21

Connecticut to Improve Officer Access to Information 22

Conferences and Events 23

Florida's Integrated Criminal History System

by Pearl Adams Terrell

Pearl Adams Terrell has been employed at the Florida Department of Law Enforcement for over 30 years and served in many different capacities during this period. Currently, she is a Government Analyst in the Criminal Justice Information Services (CJIS) program area and serves as a member of ICHS Project Management Team, assigned to coordinate the End Users' Input and Communication efforts associated with the implementation of the new Integrated Criminal History System. She can be reached at PearlTerrell@fdle.state.fl.us.

The Florida Department of Law Enforcement (FDLE) embarked on a massive initiative at the beginning of the new millennium to improve Florida's crime solving processes and technologies and to improve the delivery of services mandated by Florida Statutes. This major initiative is the replacement and integration of the current Computerized Criminal History (CCH) System and the Automated Fingerprint Identification System (AFIS) into the Integrated Criminal History System (ICHS).

Background

The Florida Department of Law Enforcement (FDLE) manages Florida's central repository of criminal history records (arrest, judicial, and custody information associated with criminal offenders) as well as the Automated Fingerprint Identification System (AFIS).

This repository is referred to as the Computerized Criminal History (CCH) system and was originally designed in the early 1970's. Florida has the third largest CCH file in the nation. The current CCH system contains criminal history records on more than 4.6 million offenders representing over 21 million criminal arrest records stored in the CCH system. These are used by

criminal justice agencies to identify suspects in criminal cases, identify repeat offenders, implement sentencing guidelines, and identify inmates. In addition, criminal records are also widely used in Florida, which is a public record state, by private and public organizations as an important part of back-

"In addition, non-criminal justice governmental agencies and the public were given an opportunity to articulate their needs for new features, since criminal history information is used outside the criminal justice community, as well."

continued on page 2

ground investigations for licensing and employment purposes. This information must be available in varying formats and degrees of completeness as needs and Florida laws permit.

Current System

The current CCH system serves as the point of contact between the State of Florida and the identification and criminal history systems at the Federal level, operated by the Federal Bureau of Investigation (FBI). Likewise, the CCH system interfaces with the corresponding criminal history systems in other states via the National Law Enforcement Telecommunications System (NLETS).

Although this dated CCH system has undergone scores of major modifications, the underlying technology (operating system, database management system, and much of the application code) has remained essentially unchanged. The current computing platform is proprietary and no longer provides FDLE with a strategic growth path, nor will the technology effectively support the functions demanded by the customers.

The AFIS was initially acquired from Printrak Corporation in the late 1980's and contains fingerprints on file of persons arrested in Florida. The purpose of AFIS is electronic storage, retrieval, and identification of fingerprints

associated with criminal offenders in Florida. Again, this information must be readily available to members of the criminal justice community. AFIS too, has undergone modification as well as technology changes over the last decade. Yet, there is a need to upgrade both the hardware and software technology of AFIS to fully integrate its interaction with the central repository of criminal records.

Launching the Project

The ICHS project itself is a statewide initiative and in order to design the most effective tool possible, FDLE recognized that it must give utmost consideration to suggestions of those who rely upon the system to carry out their organization's mission. Therefore, FDLE invited a broad range of systems users and customers to participate in numerous activities aimed at gathering information on desired features for the ICHS. The initial efforts on the ICHS project began during 2001, with the establishment of a statewide ICHS Advisory Workgroup, which consisted of operational experts and criminal justice practitioners from all entities of the criminal justice community. In addition, non-criminal justice governmental agencies and the public were given an opportunity to articulate their needs for new features, since criminal history information is used outside the criminal justice community, as well. For example, governmental agencies obtain criminal history information from the system in support of background checks on prospective



Editor

Dara Lynn Ekanger

Advisory Board

Talmage Ekanger
Greg Grajczyk
George Boos

Editorial

Assistants

Miriah Fawcett
Mary Hanson
Terri Mielitz
Jan Rollins

Design

Vision Marketing

Integration News is published bimonthly by BGL Publishing

P.O. Box 68
301 S. Main St.
Milbank, SD 57252

Phone: (605) 432-6801
Fax: (605) 432-9121
Website: www.integrationnews.com
E-mail: editor@integrationnews.com

Regular Price Subscriptions:

One year (6 issues), Electronic, \$125
One year (6 issues), Hard Copy, \$149

Promotional Offer: \$95 for Any Subscription

Five Convenient Ways to Subscribe:

E-mail: subscribe@integrationnews.com
Website: www.integrationnews.com
Phone: (605) 432-6801
Fax: (605) 432-9121
Mail: P.O. Box 68, 301 S. Main St., Milbank, SD 57252

Submissions:

Original article submissions regarding criminal justice data integration are encouraged. Please contact the editor at editor@integrationnews.com.

or current employees. Firearm dealers depend on ICHS to provide approval or disapproval of firearms purchases by individuals, in accordance with state and federal law. Lastly, the general public uses the system to obtain public criminal history records.

Utilizing the aforementioned groups and other stakeholders, FDLE conducted a series of meetings and workshops with stakeholders' groups to assist in identifying the needs, requirements and functionality for the ICHS. This comprehensive approach included a web-based survey, consensus sessions and a series of stakeholder interviews. The stakeholders' participation is an ongoing effort throughout the life of the project.

During April 2001, FDLE selected the Science Applications International Corporation (SAIC) for the Analysis phase of the project, which completed June 2002. Approximately 3,000 system requirements resulted from this effort, which reflect the needs of those that use the data and form the foundation for the design of the new system.

Design—Development—Implementation

Until April 2002, all supporting documents for ICHS reflected and presumed a single development effort—followed by an implementation in what was referred to as a turn-key “Big Bang” approach. However, due to the prudence of FDLE's internal Project Manager, this approach was abandoned. Subsequently, during April 2002, a major change occurred in the implementation approach, when FDLE determined that a less risky and perhaps more appropriate approach for this large and complex undertaking was to develop and accept the system in incremental “Builds.”

The ICHS Design, Development, and Implementation undertaking is a two-and-one-half-year effort that began on April 29, 2003, when the Florida Department of Law Enforcement (FDLE) entered into a \$37.4 million contract with Science Applications International Corporation as the prime Architecture and Integration (A&I) vendor for the project. As conceptualized, the five phases depicted in the ICHS Phase

Timeline/Schedule chart (see page 4) represent the entire Design, Development, and Implementation project. At the end of each phase, FDLE has the option of retaining or replacing the vendor; therefore, these phases essentially represent five sequen-

tial, interim projects. The first of these, Phase 1, began on April 29, 2003 and was completed October 29, 2003.

Phase 1—System Design

Phase 1 work resulted in the creation of a System Design Document (SDD) describing the master design for accomplishing the development effort to follow in later phases. The SDD allocated the system requirements to one of the four Builds.

Phase 2—Build 1

The second phase of the work will produce two products: a Bridge AFIS, which will augment the current AFIS system, and a Build 1 model, which provides a non-production demonstration of the ICHS system and is deemed non-production only. The Bridge AFIS will incorporate ICHS hardware components into the existing AFIS system to address specific suspected failure points as a means to mitigate the risk associated with the current system approaching capacity limit.

Phase 3—Build 2

The completion of the Build 2 product is the Initial Operational Capability (IOC) for ICHS. The focus of this phase will be the replacement of the legacy CCH functionality. Bridge AFIS will continue to be utilized and will be integrated into the ICHS architecture. At IOC, there will be an operational capability for participants to perform selected tasks to completion and an environment for local agencies to transition from current systems to the new ICHS. In addition, the vendor must demonstrate that the ICHS IOC can handle the required volumes and capacities of information and perform within the speed and memory standards specified for the system.

Phase 4—Build 3

The fourth phase of work will produce the Build 3 product. The Build 3 cycle will occur while there is a concurrent operation between ICHS and the current AFIS and CCH systems. Further, Build 3 will add additional critical requirements that relate to the core business functions, and will see the end user operational transition taking place.

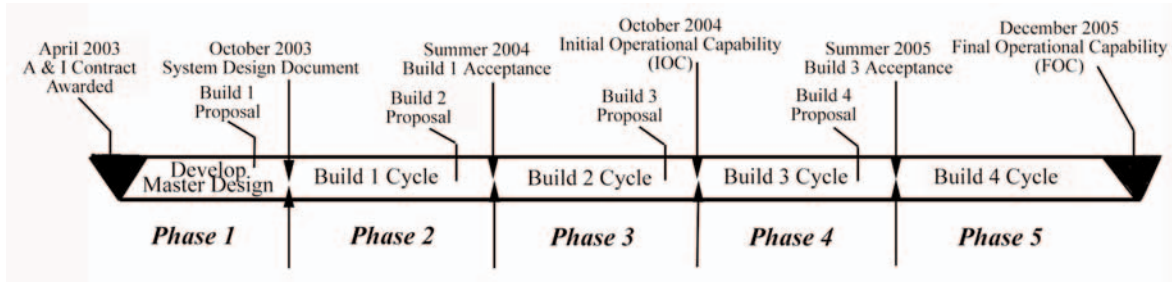
Phase 5—Build 4

The last phase of the work will produce the Build 4 product and will represent the Fully Operational Capability (FOC) for ICHS. During this phase, interfaces to additional external systems and the remaining unfulfilled requirements will be implemented.

Although not originally part of the ICHS project scope, in early 2002 FDLE began to document the need to replace/update older livescan equipment at local agencies within the scope of the ICHS project. The replacement/upgrade will be required to maintain ICHS compatibility. Finding a means to maintain the uninter-

“[At] the completion of the Build 2 product ... there will be an operational capability for participants to perform selected tasks to completion and an environment for local agencies to transition from current systems to the new ICHS.”

continued on page 4



ICHS Phase Timeline/ Schedule

rupted interface of ICHS to the livescan equipment of local law enforcement agencies is a significant issue for the project.

Bridge AFIS is the concept developed by the FDLE to ensure that fingerprint capability will be available beyond the projected failure date of the current AFIS system (currently projected for April 2005). In order to build Bridge AFIS, the FDLE has purchased ICHS production hardware earlier than planned and this hardware will host the Bridge AFIS capability. Bridge AFIS will enable local agency users to continue to use their existing livescan equipment to interface with Bridge AFIS to access ICHS fingerprint data. However, even with Bridge AFIS, some of the ICHS functionality (such as single print identification and palm print analysis) will not be available to law enforcement agencies using older model equipment. This interim Bridge AFIS capability is scheduled to be delivered as part of Phase 2/Build 1 in early summer 2004. The capability will only be in place between Build 1 completion and the completion of the final Build in December 2005. After that, agencies will have to upgrade or replace their older model livescan equipment to be able to use any of the ICHS system capabilities.

Thinking outside the box on the dilemma of the AFIS failure date presented FDLE with a unique opportunity to devise a unique resolution!

New ICHS Features

Rap (Record of Arrested Person) Sheet

The readability and presentation of the rap sheet will be improved to make it more easily understood. The new rap sheet will include the data elements covered in the national standard rap sheet that has recently been adopted for information interchange. Some of these new data elements include: drivers license number, photographs, and date-specific height, weight, hair color, eye color, and address. In addition, based on a requestor's profile, a customized rap sheet oriented to the requestor's needs may be obtained. Some examples include: rap sheets with just felonies, rap sheets with the information ordered from the last date of arrest to the first date of arrest or vice versa, and rap sheets with or without photos.



Profile

ICHS will use a profile of each individual within an agency to determine the allowed functionality and access rights or activity. The profile will contain contact information and access permissions to regulate access to functions and data throughout the system. The profile will also maintain the individual's preferences for the content, format, and method of delivery of reports (rap sheets), and information related to the billing for services, if applicable.

Searching Multiple Data Sources

ICHS will provide the capability to search multiple data sources. This is considered a time-saving strategy when numerous data sources are queried for routine activities. ICHS will allow submission of an inquiry that will provide selected information from a variety of sources without the tedium of doing queries to each source independently.

Linking Data

ICHS will provide the capability to link demographic data to each applicable arrest. Some examples of information to be collected and linked to the associated arrest include: name(s); DOB(s); height; weight; hair color; mugshot; photos of scars, marks, and tattoos; address; and occupation. This will allow a view of the changes to a subject over a period of time if multiple arrests occur.

Suspect Lineups

ICHS will provide the capability to provide photo lineups of possible suspects when ICHS records include mugshots. This will assist investigators in identifying suspects.

Elimination Prints

ICHS will provide the capability to submit and retain elimination prints from a crime scene and other emergency response personnel when applicable laws allow it. This will help avoid potential misidentification of suspects.

Offender Information

ICHS will provide the capability to enter information regarding items worn or carried by an offender at the time of arrest, and a text description of tattoos. Both of these are searchable elements useful for investigations.

DNA

ICHS will provide a notation that a DNA sample is already available for the subject, which prevents duplication of samples. There will be a reduced need for costly supplies and labor used for DNA testing and an overall reduction in duplicate processing. Cross references within the criminal history showing a DNA sample is on file along with fingerprints will provide additional reliability to the submission and identification process.

Barcode Printer

After a single fingerprint identification of a subject from whom a DNA sample needs to be collected, a barcode of the state identification number for the subject will be available for inclusion on the label that must be printed and attached to the DNA sample. The barcode printer may be used wherever the sample is taken.

Identity Theft

ICHS will provide the capability to verify a confirmed identity theft victim based on fingerprints. On a voluntary basis, an identity theft victim may be fingerprinted to have fingerprints stored in a database available to law enforcement agencies for positive identification.

Images

A camera will capture a mugshot of the individual as well as photographs of scars, marks and tattoos. A digital image of these photographs may be submitted to ICHS for inclusion in the individual's record. These images provide the basis for subsequent automated lineup capabilities within ICHS.

Fingerprint Capture

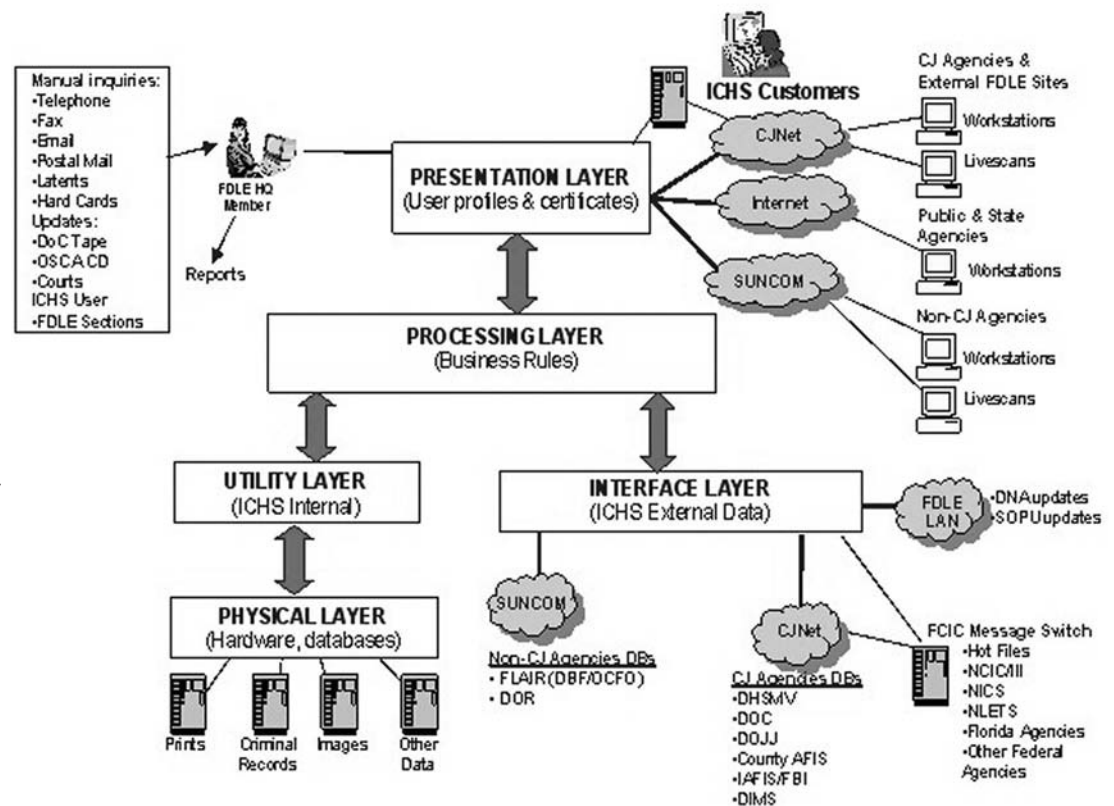
A livescan device can capture all ten fingerprints as well as palm prints for entry into ICHS or identification of the individual. Both rolled prints as well as slap prints may be collected on this device. These livescan devices can also interface to a printer to produce a hardcopy record for retention needs. This device may be used in several locations, which include courtrooms for the capture of ten prints from individuals appearing due to a Notice to Appear, Summons or direct files

where fingerprints have not already been submitted for this case to establish an ICHS record.

Rapid Identification

A rapid identification device will allow a single fingerprint (either a rolled or flat print) to be captured and used to provide rapid and positive identification of an individual. Demographic information (e.g., name) and an associated fingerprint will be used to confirm the identity of the individual subject. An input device, such as a PC or a magnetic stripe reader, would be necessary to capture the demographic information. Rapid identification techniques have a number of potential applications. These include:

- Courtrooms to confirm the identity of the defendant. This includes first appearances.
- Clerks of Court to assist in insuring that disposition information is associated with the correct individual.
- Prisons, detention centers, jails, etc. for processing individuals as they enter or are released. This can also be used for prisoner movement.
- Probation offices to allow probation officers to confirm the identity of probationers.
- Patrol cars for on-site identification.



ICHS Conceptual Architecture

continued on page 6

Among the many benefits anticipated with the New Integrated Criminal History System are the capabilities to:

- Improve the rate of dispositions, on-line and without paper submission from Florida's Clerks of Court.
- Reduce processing time for the creation of and updating of criminal records.
- Increase accuracy of records through automation and single entry at the data source.
- Continue Florida's goal of meeting the timetables for criminal history record completeness.
- Improve the presentation and readability of rap sheets, including implementation of the national standard rap.
- Create the ability to allow links to hot files (protective orders, domestic violence, arrests, warrants and conviction information) to improve access to protection orders and records of subjects wanted for stalking and domestic violence.
- Allow the submission of images including mugshots, scars, tattoos and other features that will assist in investigations.
- Allow the submission of information regarding persons given Clemency by the Office of the Governor that are necessary to determine if the right to possess firearms has been restored.
- Support high volume on-line transaction processing to meet the growing needs of the criminal justice community.
Florida has over 51,000 devices, representing over 1,000 criminal justice agencies with access to the network. In addition, more than 2 million non-criminal justice checks are conducted each year.
- Improve integration between criminal history information, fingerprint images, and photographic images.
- Allow the submission of commitment information on-line and automated from the Department of Corrections, with fingerprint images to support positive identification of incarcerated offenders.

"FDLE believes that it is more cost-effective to build a system that is modular in design, to avoid totally reengineering when there is a need to install additional components to the existing system."

- Create the foundation for a truly integrated criminal records system that is flexible to meet the growing and changing needs of our customers in Florida and nationally.

Lessons Learned

If an organization is anticipating managing a large, complex project, consideration should be given to dividing the project into smaller tasks that can be associated with contractual deliverables.


- The vendor's incremental payments should always be associated with contractual deliverables.
- Break vendors' proprietary hold on system software and hardware and create competition among vendors for cut-rate prices.
- Based on past experiences, FDLE believes that it is more cost-effective to build a system that is modular in design, to avoid totally reengineering when there is a need to install additional components to the existing system.
- Early involvement of stakeholders is critical to the project's success and is essential for change management.
- In the area of management of expectations, it is critical to ensure that customers, policy makers, and the vendor clearly perceive "success as success."
- During the Analysis phase, it is often difficult for staff to share business rules about each function when the staff is very familiar with a routine. Staff must communicate these rules in detail while guarding against the risk of recreating your existing system.
- Involving a wide range of system users, with a variety of disciplines, will minimize misunderstandings during the Analysis phase and will result in more accurate and complete system requirements.
- While attempting to establish a timeline for a project of this magnitude, it is wise to factor in time that may be required to settle a dispute after the contract award.

Summary

The ICHS is expected to be fully operational by December 2005, with an Initial Operational Capability currently scheduled for October 2004. This major initiative is expected to improve the delivery of services mandated by Florida Statute and will include direct support for local agencies' activity as a major component of ICHS. At the Final Operational Capability, FDLE's ICHS vision will be implemented:

- A modular, integrated system providing online access to a person's complete criminal history, based on positive biometric identification

- A high-volume, transaction-based system, using single data entry to provide integrated, unambiguous, quality-assured multimedia data
- A system providing enhanced accessibility and dissemination of criminal justice information to the public and criminal justice community through seamless integration with local, state, and federal systems
- A criminal justice information system that is more responsive and cost-effective

For more information on the ICHS project, readers may email the staff at ICHS@FLCJN.net or view the ICHS website at www.fdle.state.fl.us/ICHS/. 



MATRIX Loses Two States

Project Matrix (Multistate Antiterrorism Information Exchange) lost two more states in January amid concerns of privacy, cost, and data security. Utah and Georgia, both starter members of the intergovernmental criminal tracking and identification project, pulled out, joining six other states that have withdrawn in the last six months.


Gov. Olene Walker put a hold on Utah's participation January 29 and formed a committee to assess the security and social implications. Georgia Gov. Sonny Perdue pulled his state out on January 30, a few months after his attorney general stated that sharing drivers license and vehicle registration information violates state law.

Membership in Project Matrix costs states \$1.7 million a year for licenses to access the system. That is in addition to as much as \$130,000 to build the necessary infrastructure to become a node on the Regional Information Sharing

Systems (RISS), a secure intranet that connects to a super-computer hosted by a Seisint Inc.

Jeffrey Hunker, a former senior director for critical infrastructure at the National Security Council stated, "A network of information sharing and data mining among law enforcement is both appropriate and inevitable. What I don't see with Matrix is a system of checks and balances." Such checks and balances are necessary in an age where privacy and data security are prime considerations.

Project Matrix was started in January 2002 by the Justice and Homeland Security departments.

For more information visit: <http://informationweek.com/story/showArticle.jhtml?articleID=17602295>. 

Case Study: Using XML for Alaska Criminal Justice Data Exchange

by Steve Horneman and Nancy LaPlaca

Steve Horneman has over 11 years experience in the IT and software industries. Prior to becoming the Director of Marketing for XAware, Inc., Steve served in various leadership capacities at DEC, Quantum and Compaq. He has been instrumental in growing XAware's Criminal Justice Integration Practice. Steve is a graduate of the University of Colorado in Marketing, with an MBA in Finance. He can be reached at shorneman@xaware.com.

Nancy LaPlaca, J.D., worked on justice integration issues for the State of Arizona for five years for the Arizona Supreme Court and the Criminal Justice Commission. She helped develop Arizona's statewide criminal justice data dictionary and common charge table, drafted statute and rule changes to improve reporting, and worked with counties to determine criminal justice business process flows. Nancy's private sector experience includes criminal justice consulting with Sybase, Inc. and XAware, Inc. She can be reached at nancy@xaware.com.

XAware, Inc. is a worldwide leader in XML enablement, data integration, and information exchange. From a single point of access, users can query, view, and update information from dozens of data sources. XAware's drag-and-drop environment reduces the need to write complex custom code to retrieve, translate, manipulate, and exchange information. XAware utilizes web services and can implement Justice XML. XML "views" of data from different systems can be created, updated, and then decomposed and sent back to the original data source.

The State of Alaska used SEARCH's JIEM (Justice Information Exchange Model) tool to map out thirty-six exchanges. Rather than continue mapping hundreds of exchanges, Alaska hired XAware to help implement an XML-based exchange between the Court and Public Defender for Notice of Appointment of Counsel. Implementing this exchange took XAware and Alaska three days.

Every justice agency in the U.S. is acutely aware of the lack of electronic data sharing. Over the past two decades, approaches to sharing justice information have changed dramatically. Integration efforts have included point-to-point, proprietary interfaces, centralized repositories and, most recently, a network-based approach. Traditionally, interfaces were brittle, meaning custom code was required, and re-writing was required if any agency changed applications or database. Some jurisdictions find data repositories a

necessary part of their IT infrastructure. Statistical analysis may require that persistent data be available. However, data repositories have ongoing maintenance costs, technologies can become out-of-date, and system performance issues are common problems. Bulk porting of data sets is often necessary.

Most recently, agencies have begun considering network-based integration. Users access information on-demand, and stakeholder agencies maintain ownership of data. Network-based integration using XML can include a data warehouse, but data persistence is not required. XML-based integration uses standardized protocols like SOAP (Simple Object Access Protocol) and WSDL (Web Services Description Language) to exchange information over the web.

Justice XML

Justice XML is the common articulated language that drives a network-based approach. The standards created by Justice XML allow agencies to exchange information in a platform-, application- and vendor-neutral environment.

Justice XML was created by the U.S. Department of Justice (DOJ) and Georgia Tech Research Institute. IJIS, the Institute for Justice Information Systems, is a non-profit organization dedicated to helping justice agencies make the best use of technology to share information. The Global Justice XML Data Dictionary Schema (GJXDDS) was first released in June 2002. Both DOJ and IJIS have embraced XML as the best technology to quickly achieve interagency exchanges.

Justice XML is standardizing data elements and documents and developing schema for rap sheets, court filing records, driver records, arrest warrants, charging documents, and potentially hundreds of other documents. For more information, see: <http://it.ojp.gov/initiatives/files/JusticeXMLStructureTaskForceReport.doc>.

Global Justice XML Data Dictionary (GJXDD) work groups are developing common, well-defined data elements. The GJXDD group recognizes that the full schema is very large and over-inclusive, and that many agencies will only use a small percentage of the elements. They are working on a tool that will allow agencies to pick and choose parts of the schema. Some customization of schemas will also be allowed. For example, an agency could restrict the field length for a name to 30 characters, or filter out codes like

the National Crime Information Center's (NCIC's) long list of vehicle codes. Unique, local components could also be added as long as they fit GJXDD guidelines. GJXDD can be found at: www.it.ojp.gov/jxdd/prerelease/3.0.0.1/JusticeXMLDataDictionary.pdf.

The DOJ's goals for Justice XML are to maximize data sharing, object reusability, and extensibility, easy maintenance, and employ current technologies and best practices—for free! Although adoption of Justice XML is voluntary, it will eventually be the standard for all justice agencies.

What Are Web Services and Service-Oriented Architecture?

Web Services Overview

Web services are loosely coupled software components delivered over Internet standard technologies. They enable enterprises to create interlinked, interactive systems that can communicate in a common dialect with each other. Web services are defined by three XML-based components: Universal Description, Discovery, and Integration (UDDI) for registering and discovering web services, Web Service Description Language (WSDL) for contacting/specifying the details of the service to be provided and describing the communication between the provider and the user, and the SOAP protocol for actually carrying the message and carrying out the procedure call aspects on all interactions.

“Network-based integration using XML can include a data warehouse, but data persistence is not required.”

SOAP defines a uniform way of passing XML-encoded data. It allows remote procedure calls using HTTP (Hyper Text Transfer Protocol), allowing communication via the internet between remote systems. The internet is the physical network infrastructure, and SOAP is used to communicate XML messages via HTTP.

Service-oriented architecture has been around for some time, but until common standards like XML, SOAP, and WSDL existed, there was no practical way to use it. XML, SOAP, UDDI, and WSDL are interoperable and platform-neutral.

Web services run over HTTP and TCP/IP networks, just like web pages. Integration using XML and web services can be implemented one exchange at a time. XML's revolutionary premise is that data can reside anywhere: in a database, web pages, flat files, spreadsheet, etc. An XML message is converted to a request that the data source being queried can understand, and the results are converted back to XML. The programming and processing are transparent and take place in a web server.

What's so Great About Web Services?

The real value of web services is that its benefits are both immediate and long-term. Immediate benefits include rapidly implemented data exchanges, a one-exchange-at-a-

XAware's secure network-based information sharing approach

Key Features of XML-Based Integration	Key Features of MXL-Based Integration
- COTS and industry standards-based approach to justice information sharing	- Simpler and more cost-effective than point-to-point and data warehouses
- Information Exchange from any application or database, on any platform, to any client	- Flexible and scaleable - as standards evolve and project scopes change
- Full bi-directional access with query, push, pull, publish, and subscribe	- Original and target data can be updated or returned in initial state
- Synchronous or asynchronous transfer protocols based on events or triggers	- Authentication, authorization, and encryption
- Full support for XML, Justice XML, and Web services	- Complete consulting, customization, and implementation services available

continued on page 10

time approach, and reuse data of XML objects. Once an object is created, it can be added to a library of “create-once, use-many” XML objects, and served to any data source that can process XML. Object reuse means that as each successive exchanges use objects already in the library, the cost to build each exchange goes down.

Objects are called “loosely-coupled” because the object is independent of the source. This allows agencies to easily change vendors or technologies by re-mapping the data objects to the new source. Since program logic calls the object—and not the source—there’s no need to change the object if the source changes. If an agency changes its application or database, a simple re-mapping to the new data source is all that’s needed.

Using Web services for data source access rather than hard-coded logic adds flexibility. The client data source(s) can know less about the system accessing it, and must

Prosecutor’s Office, Public Defender Agency, University of Alaska Justice Statistical Analysis Center and the National Law Enforcement and Corrections Technology

Center–Northwest (NLECT-NW), to look at how to best achieve interagency information exchanges. The team submitted a charter to the Criminal Justice Information Advisory Board (CJIAB) for MAJIC (Mapping Alaska’s Justice InterChanges). Alaska Statute 12.62.100 requires that the CJIAB advise DPS and other justice agencies on developing and operating criminal justice information systems. The project obtained approval by the CJIAB Chair and MAJIC began.

“Law Enforcement and Corrections (LE&C) officers in Alaska and other remote areas of the United States face unique challenges to crime prevention, investigation, and rehabilitation efforts.”

The National Law Enforcement and Corrections Technology Center—Northwest

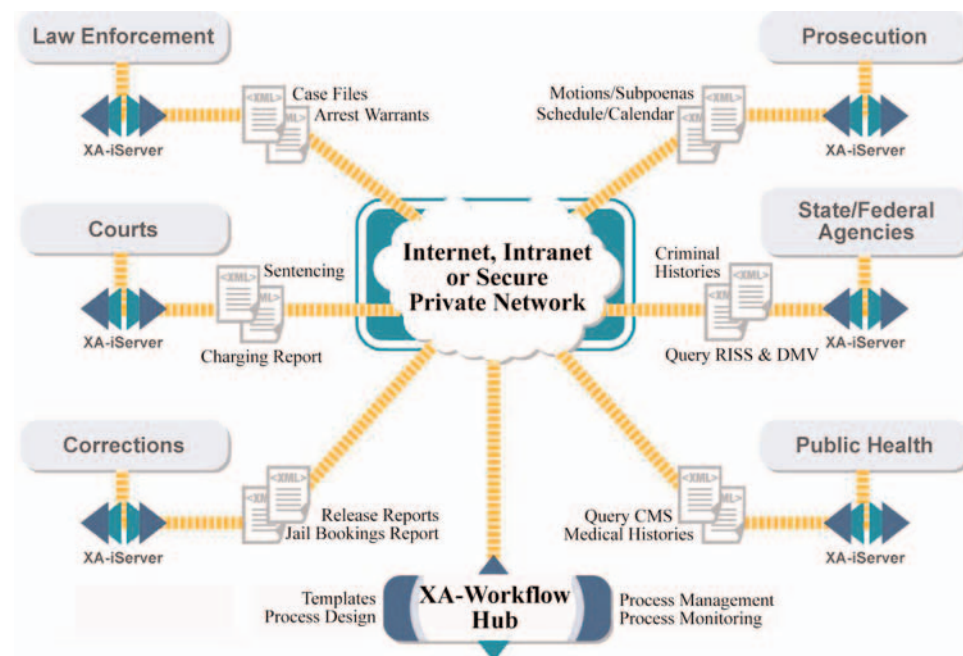
Law Enforcement and Corrections (LE&C) officers in Alaska and other remote areas of the United States face unique challenges to crime prevention, investigation, and rehabilitation efforts. NLECT-NW was established to provide assistance in defining LE&C’s requirements for information and operational technology, with specific

attention toward technologies that support law enforcement and corrections under the extreme weather conditions and vast distances of rural Alaska and other parts of the United States.

A program of the National Institute of Justice, NLECTC-NW was founded in 2001 in partnership with Chenega Technology Services Corporation and identifies, evaluates, demonstrates, and assesses technology applications for state and local law enforcement and corrections agencies.

Staff at the NLECTC-NW partnered with MAJIC team members to assist in the location of technologies, training, and tools to assist in the mission of achieving

criminal justice data integration across the state. Because of the far-reaching impact of this mission, NLECTC-NW has made support of this group a priority since its inception, both in funding and in providing staff.



only be able to decode the XML stream and use SOAP messages. Modifications are much easier than developing application-specific interfaces.

Alaska Creates MAJIC

In July 2002, the State of Alaska organized a team of criminal justice personnel from the Alaska Court System, Department of Public Safety (DPS), Anchorage Municipal

After a two-day training session, the team began modeling exchanges—identifying the agencies, documents, events, and conditions involved in each exchange. The

team initially thought that the entire universe of exchanges should be mapped before implementation, but later decided that more value would be achieved by demonstrating the effectiveness of JIEM by implementing a proof of concept exchange using XML. Thirty-six exchanges were documented for the proof of concept.

The Alaska team decided to use an XML and Web services-based architecture, which allows bi-directional exchanges—the ability to select and extract data from one agency's database and insert it into another agency's database.

The Institute for Justice Information Systems Recommends XML

IJIS, the Institute for Justice Information Systems, is a non-profit organization dedicated to helping justice agencies make the best use of technology to share information. IJIS is part of a project sponsored by the Global Justice Information Sharing Advisory Committee (GAC), under the U.S. Department of Justice (DOJ). GAC is charged with facilitating standards-based electronic information sharing within justice and law enforcement. The broad scope is essential, since eventually information will be shared by a large number of agencies, from police to prosecutors to motor vehicles agencies. In June 2002, the group produced the Global Justice XML Data Dictionary Schema (GJXDDS). The Global Justice XML Data Dictionary (GJXDD) specification includes a Data Dictionary, XML Schema and Data Model. This means that each justice agency—whether law enforcement, courts, prosecution, defense, corrections, probation, motor vehicles or any other interacting agency—will utilize a common description of data elements.

MAJIC's Exchange between the Courts and Public Defender

For the proof of concept, the MAJIC team chose an exchange between the Alaska CourtView application and the Public Defender Agency, requiring bi-directional exchange between an NT and Novell network and SQLServer 2000 database to Access97. The proof of concept was for a single location handling over 2,500 exchanges. When fully implemented, more than 15,000 paper and manual appointment of counsel exchanges that occur each year between these agencies will be automated.

The MAJIC team had expected to spend hundreds of thousands of dollars just mapping exchanges. However, JIEM allowed the project team to efficiently accomplish mapping and Alaska hired XAware to implement exchanges for a fraction of the estimated project budget.

MAJIC's future goals include implementing a second, more complex project, perhaps mapping exchanges involving Conditions of Release (bail conditions). Currently, this process is entirely manual, leaving law enforcement and other agencies without online access to critical information about release conditions. The Alaska Court system is poised to automate distribution of this data as part of its court application implementation. Once the proof of

concept project is implemented in the initial court location, the Public Defender Agency and courts intend to refine and expand the exchange to other court locations.

XML Exchanges: How Do They Work?

XML drag-and-drop tools create on-demand views of many different agency data sources, including bi-directional exchanges—essentially allowing one to extract from one data source and insert into another. An XML integration server can process data from internal systems to any outgoing XML schema and process inbound XML schemas to any number of internal systems without the need to write code. Information from many different sources can be aggregated into a single XML view.

Connectivity to other agencies, such as Motor Vehicle records can be added as needed. XML-enabling legacy systems using traditional custom code can be expensive and risky.

Security

The exchange XAware implemented includes XAware authentication, authorization and encryption by utilizing the existing capabilities within typical customer application server environments. End-user authentication is provided by use of an ID and password on the presentation layer. Authentication is provided by passing the appropriate credentials in the Web services request. HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) provides 128-bit encryption, essential for passing justice information over the Internet.

"XML drag-and-drop tools create on-demand views of many different agency data sources, including bi-directional exchanges—essentially allowing one to extract from one data source and insert into another."



A Report to Congress on the Information Sharing Needs & Requirements of the Office of the Sheriff

**A White Paper
Prepared By
the Pegasus Research Foundation
Dr. Lee Colwell**

Dr. Lee Colwell is the Executive Director of the Pegasus Research Foundation. He was formerly Associate Director of the FBI, and is a nationally recognized leader in local, State, and federal law enforcement policy development and implementation.

The Pegasus Research Foundation ("PRF") is a non-profit corporation created to work in coordination with the Nations' Sheriffs, municipal police, fire departments, first responder, public health, and critical infrastructure entities, to facilitate multi-state sharing of essential law enforcement and Homeland Security information. The following piece is a reprint of a report to Congress on the information sharing needs and requirements of the Office of the Sheriff. It was prepared by Dr. Lee Colwell, of Pegasus Research Foundation, and submitted to Congress in October 2003. It urges Congress to consider the need for nationwide information sharing capabilities for local law enforcement and other essential front-line responders, and the dramatic impact that has on homeland security. It also addresses a concern of Congress regarding, "information sharing initiatives that are being developed independently, with no apparent plan to integrate them with other systems operated by Federal law enforcement and with RISS and LEO."

Background

The problem of inadequate data interoperability—simply stated, computer systems that are not integrated and, accordingly, "do not talk to each other"—plagues Sheriffs' Offices and all other government agencies at the local level, just as it plagues the Federal and State governments and corporate America. However, this problem is laden with critical policy implications when the systems at issue are integral to the Nation's crime fighting and homeland security efforts. While law enforcement agencies primarily investigate crime and provide an ever-increasing array of services to their constituents, law enforcement agencies now are also central to preventing terrorist activity within the United States. Even so, the vast majority of our front-line law enforcement personnel have not yet been engaged in any nationwide information sharing effort: the Hart-Rudman Report emphasizes that "650,000

local and state police officials continue to operate in a virtual intelligence vacuum." These facts underscore the critical policy relevance of two indisputable facts which of necessity must be central to any nationwide plan for information sharing: first, the next terrorist act in the United States will occur within the jurisdiction of a Sheriff; and second, Sheriffs have more than their fair share of the same communications and data interoperability problems plaguing agencies at all levels of government.

To address these two points, the NSA Pegasus Program has been planned and developed in coordination with the FBI Law Enforcement OnLine (LEO) and the Regional Information Sharing System (RISS) programs. For more than two years, executives of NSA Pegasus, LEO and RISS have been in constant contact, proceeding with a plan for the accomplishment of their distinctly different missions. NSA Pegasus has committed to utilize existing LEO/RISS communications infrastructure if that is the most economical route. Further, NSA Pegasus and LEO/RISS representatives have been coordinating for NSA Pegasus to meet information sharing needs that LEO/RISS do not plan to meet.

"As a representative to South Carolina's Homeland Security Council, there is one constant concern—lack of communications through information sharing."

***Sheriff Lee Foster
Sheriff, Newton County, SC
Representative, SC Homeland Security Council***

Critical here is the fact that, except for NSA Pegasus, no Federal, State or other agency, program or institution has as its mission a national plan to address problems of inadequate data interoperability between Sheriff's Offices, municipal and tribal police agencies, fire departments, first responders, public health offices, water and electric

utilities and other critical infrastructure local level government and private sector entities. In fact, the Nation's Sheriffs, who provide law enforcement and public safety services ubiquitously throughout the Nation, believe that only the NSA Pegasus Program has precisely this planning vision.

With strong Congressional support in FY02 and FY03, NSA Pegasus has begun integrating and providing access to local law enforcement databases throughout the Nation, databases that LEO/RISS do not access and do not plan to access. Local agency database integration and access, across both State and local jurisdictional boundaries and multiple sector "stovepipes", is the principal mission of NSA Pegasus, complemented by efforts to advance nationally-embraced

information sharing standards built on Federal policies and standards. The NSA Pegasus Program will continue to carry out its mission and plan with continued Congressional support in FY04 and beyond.

The Problem-Inadequate Data Interoperability at the Local Level

One of the essential elements of our Nation's structure of government, and one of the key components which gives our republic its strength, is that most law enforcement, criminal justice and public safety authority and responsibility is carried out by local agencies, rather than by Federal or State agencies. As such, local agencies have the vast majority of the front-line personnel actually involved in critical, structural, frontline law enforcement, criminal justice and public safety responsibilities. At the same time, these local agencies, especially small and rural agencies, are also the least funded, least equipped and least prepared to deal with the implications of rapid technology changes. And, the fact is that rapid technology changes fundamentally impact local agencies' conduct of their missions, none more so than the profound communications and information technology innovations that have emerged over the past decade.

In recent years, many of the Nation's law enforcement, criminal justice and public safety planning efforts have been Federal or State top-down initiatives, focusing on wholesale solutions from a Federal or State perspective. These top-down approaches, while important in looking at the problem from the Federal or State perspective, do not, and structurally cannot, really focus on identifying and responding to the front-line needs of local agencies. Nor do top-down approaches empower local agencies: all too often, local agency "buy-in" and commitment, which is so critical to successful implementation at the local level, is ignored.

Since the events of 9-11, widespread national consensus has emerged over the law enforcement and homeland security need for information sharing. A critical component of this information sharing is "data interoperability" or "integration"—computers that in fact "talk to each other." Solving the data interoperability problem is not only vitally important for local law enforcement to carry out its traditional day-to-day operational mission, but has now taken on grave new significance as local law enforcement, since 9-11, has taken on new homeland security responsibilities.

A variety of law enforcement initiatives are being advanced to solve some aspect of the problem of law

enforcement data interoperability. Many of these initiatives are primarily regional in nature, intended to solve the problem for a designated local region. Additionally, there are several information sharing initiatives at the national level; however, these national initiatives are primarily data

communications networks that assume that necessary and accessible local databases, and the computers and network connections necessary for those databases to be accessed, exist at the local level. Stated differently, even though the need for access to local agency databases is an absolute necessity for local agency information sharing, it is not the mission of any other national law enforcement information system initiative, including LEO/RISS, to address the lack of integrated interoperable databases at the local agency level.

From a policy standpoint, the proper role of the Federal government in solving communications and information sharing problems in State, local, and tribal

systems is to encourage, support and facilitate the design and implementation of "enterprise-wide" technology solutions. That is, the Federal role is not to mandate technology design, but rather to offer planning, support and guidance from a national perspective. This kind of meaningful Federal coordination and support is critical to the development of integrated local law enforcement, first responder and critical infrastructure sector information systems within an "enterprise framework": a broad, yet defined, set of principles, standards, and policies for nationwide integration of inherently local, non-Federal and non-State, systems.

Local level information sharing requirements for law enforcement, public safety and homeland security extend beyond government agencies to others, including the private sector. Many studies and commissions have pointed to the need for information sharing, not just with and between government agencies but also with and between those private sector entities with critical infrastructure assets and responsibilities. For example, after fifteen months of evaluating the Nation's critical infrastructures, assessing their vulnerabilities, and deliberating assurance alternatives, the President's Commission on Critical Infrastructure Protection concluded that "information sharing is the most immediate need", reasoning that increasing the sharing of strategic information within each infrastructure, across different sectors, and between sectors and the government, will greatly assist efforts of owners and operators to identify their vulnerabilities and acquire tools needed for protection.²

"... prior to 9-11, had a real-time data-sharing system between rural law enforcement, state and federal agencies been in place—those routine traffic stops involving the terrorists may have resulted in their detention and perhaps prevented the 9-11 tragedy".

*Sheriff Wm. T. (Tommy) Ferrell
Sheriff, Adams County, MS
Chairman, NSA Pegasus
Advisory Board*

The Federal Response to Inadequate Data Interoperability

The United States Department of Justice presents a compelling case study of the proactive Federal response taken in light of the events of 9/11 and in response to the challenges presented by the lack of data interoperability among Federal systems. In March 2002, the U.S. Attorney General named a DOJ Chief Information Officer with a strong mandate to provide leadership in DOJ's Information Technology (IT) planning and implementation. To carry out the Attorney General's mandate, the DOJ CIO was allocated several major responsibilities. Among these responsibilities are the promulgation of Departmental IT policies, processes, and standards, and formulation of DOJ IT strategic plans. The still-new DOJ IT Strategic Plan, in turn, identifies eight overarching strategic goals that the Department will pursue in support of its new post-9/11 mission. In addition to the first goal of protecting America against the threat of terrorism, another DOJ strategic goal is to prevent and reduce crime and violence by assisting State, tribal, local and community-based programs.

The DOJ IT Strategic Plan acknowledges that Information Technology is fundamental to meeting all DOJ strategic goals: that is, IT has become an integral part of Departmental mission accomplishment. This is because DOJ IT provides an improved capability to identify, apprehend, and prosecute criminal suspects, and will also enhance Departmental gathering, analysis, and sharing of intelligence information. In addition, under the DOJ IT Strategic Plan, DOJ IT provides the communications and computing infrastructure that ensures continuity of operations and rapid response in times of crisis.

Notwithstanding this kind of proactive Federal response to integrate Federal databases, work on the complete task at hand has hardly begun. Information still exists in various databases spread among Federal, State, and local entities. In many cases, these computer systems cannot share information across the same level of government or between Federal, State, and local governments.³ Databases used for law enforcement, intelligence, and public health are not connected to recognize information gaps. As a result, agencies storing information, such as a "watch list," have not been able to thoroughly share that information with other agencies.

Efforts to Achieve Data Interoperability at the State and Local Levels

Except for the scale of the problem and the resources available to address it, problems identical to those addressed by the DOJ IT Strategic Plan also exist at the State and local

levels of government. Numerous State and local agencies maintain databases that entities in other states cannot access. The Department of Homeland Security (DHS) recognizes these issues and intends to leverage America's leading-edge information technology to develop an information architecture that will effectively secure the homeland.⁴ In addition, many State governments are taking steps to address these problems, having the scale at the State level to meaningfully do so.



Historically, State and local level responses to this kind of national problem at the State and local level have been driven by Federal legislative support for State and local criminal justice initiatives. Since 1968, Federal legislative initiatives have addressed civil uprisings, juvenile justice, multi-jurisdictional drug crime, victims' rights and assistance, violence against women, and community oriented policing.

Funding for information technology equipment, training and technical assistance is available through a variety of U.S Department of Justice (DOJ) programs, most notably the COPS Program, the Local Law Enforcement Block Grants Program, the Byrne Program, and the Juvenile Accountability Incentive Block Grants Program. Traditionally, funding from these programs has been "program-" or purpose-specific, focusing on the problems of a single information "stovepipe." The next step, presently facing the Nation, is to integrate these information "stovepipes" at the State and local level, so that the information, and the investments which have been made in these systems, may be extracted and put to work for law enforcement, public safety and homeland security.

Consistent with this historical Federal role, the DOJ Office of Justice Programs (OJP) has served as a resource supporting the development of information systems that enable the appropriate sharing of State, local, and tribal agency information. Supporting the endeavors of the justice community to electronically share information is the focus of the Global Justice Information Network Advisory Committee and the OJP and COPS technology initiatives described in this document. In this connection, OJP Fiscal Year 2000 and 2001 IT initiatives supported state, local, and tribal integrated justice systems, and in FY 2001 and 2002, OJP supported projects in eight broad areas of concentration:

- State and local government standards to facilitate the appropriate sharing of information across organizational boundaries;
- An IT website to support state and local government efforts to build integrated information systems;

- Privacy initiatives to provide policy guidance, principles, impact assessment capabilities and guidelines for public access to justice-related electronic records;
- Strategic planning for accomplishing information sharing initiatives at state and local government levels;
- Technical assistance and technology assistance to state, local and tribal agencies of the justice community;
- Project management education and training for project managers of information sharing initiatives;
- Governance models for state and local governments;
- Shared initiatives with non-traditional associates from state and local government and industry, working toward common objectives affecting the justice community.

As a result of Congressional support carried out through OJP Programs, OJP has funded a significant number of local law enforcement information sharing regional clusters, usually contained within State or Congressional districts, and local agencies themselves have also funded such regional clusters. These regional clusters, some in place and some still under development, now represent the foundational elements for a national plan for local agency information sharing through local agency database integration. That is, these regional clusters need a common platform for sharing their own information beyond their regional boundaries, both with other regional clusters, with rural agencies that may never be part of such a regional cluster, and with authorized Federal and State agencies. The NSA Pegasus Program was designed to build on and enable information sharing across State and regional boundaries, across multiple sector “stovepipes,” and with and between all levels of government, specifically including small and rural local agencies which are least equipped to control their own IT destinies, but which often serve as the Nation’s front-line responders for law enforcement and public safety.

In parallel with the DOJ IT Strategic Plan, the NSA Pegasus Program also reflects Sheriffs’ recognition of how Information Technology must now be applied, a fundamental reorientation for many Sheriff’s Offices. That is, Sheriffs recognize that IT will: no longer be a support service, but an “active catalyst for change and a direct contributor to mission accomplishment;” no longer be decentralized to support individual agencies, but an “integrated, cohesive

endeavor that builds on shared mission requirements and fosters a collaborative mission environment;” no longer be “only reactive, matching technology to an identified public safety need, but also proactive.” As such, the NSA Pegasus Program has given the Nation’s Sheriffs a strategic foundation upon which to build local agency momentum toward achieving local agency data interoperability, nationwide, and across multiple sectors.

The Underlying Causes

While there are many causes for the problem of inadequate data interoperability at the local level, two factors are underlying causes. One of these factors is a lack of local agency funding: for a great number of local agencies, there has long been a lack of sufficient funding, often due to a small, static tax base. As a result, thousands of local agencies have for years been unable to create and maintain the

computer systems and databases inherently required for integrating databases. The resulting lack of equipment, software and trained personnel has been compounded by the second cause: a lack of nationally-embraced standards for such systems and databases, established with meaningful input from their ultimate users.

“Why reinvent a new database when you can utilize the databases each agency already uses and likes?”

***Thomas N. Faust
Executive Director
National Sheriffs’ Association***

It is highly relevant that more than 18,000 law enforcement agencies and 35,000 fire and emergency medical agencies operate in the United States. Of necessity, the vast majority of these agencies purchase communications equipment independently of each other,⁵ and the same is true of IT systems. Due to the lack of nationally-embraced standards for systems and databases, the ability to share information in real time rarely exists between these agencies.

The lack of nationally-embraced standards for linking local agency information systems has also been substantially responsible for the high costs involved with data integration and has contributed significantly to the associated difficulties of exchanging data between local agencies. Because a number of organizations are currently acknowledging the importance of local agency data integration standards, it is also becoming critical that the adoption of data integration standards take into account emerging technologies, which will serve as the basis for automated data exchange. With continued Congressional support, the NSA Pegasus Program will continue its efforts of advancing nationally-embraced automated data integration and data exchange standards, built on Federal policies, standards and guidance, driven by “bottom-up” support from local agency users.

The Need

Federal Leadership and Support for Information Sharing Between and Among All Levels of Government and the Private Sector, for Homeland Security

Although the nature of American society and the structure of American governance make it impossible to achieve the goal of a secure homeland through Federal Executive Branch action alone, the Federal government must lead the Nation's homeland security efforts. The requisite Federal leadership involves shared responsibility and partnership with the Congress, State and local governments, the private sector, and the American people.

At the same time, Federal support of information sharing must address not only information sharing within the Federal government, but also information sharing between Federal, State, and local governments, and private sector organizations. The President's FY04 Budget proposed \$722 million for improvements to information-sharing within the Federal government and between the Federal government and other State and local governments. Such technology investments will improve the performance of agencies in preparing for, detecting, and responding to threats to homeland security.⁶

It is important to note that, other than the NSA Pegasus Program, no national initiative addresses the need for interoperable local agency databases. The NSA Pegasus Program, on the other hand, is designed precisely to meet that need. Without the basic building block of the kind of local agency "buy-in" commitment which is represented by the NSA Pegasus Program, local agency information sharing cannot occur, either in support of traditional local operations or in support of the National response to the terrorist threat.

A Cohesive and Responsive Approach to Local Agency Data Interoperability, Especially Focusing on Small Departments and Underserved Rural Areas

How information is to be shared by Sheriffs and other local agencies is impacted by many variables. For instance, Sheriffs, police, courts, and other agencies in rural areas work together more closely than their counterparts in urban areas. Sharing computer networks may also be a more compelling solution for local law enforcement agencies in rural areas with low tax bases and scarce resources. One size won't fit all, due often to circumstances well beyond the control of the Sheriff or local agency, or the community. This point is emphasized by the Hart-Rudman Report of an Independent Task Force

sponsored by the Council on Foreign Relations⁷, which states, "Given the size and complexity of the American society, there are no 'one-size-fits-all' approaches to addressing the nation's most serious homeland vulnerabilities."

Many rural agencies and departments have small tax bases and very scarce resources. Of the 3,088 Sheriffs'

Offices nationwide, approximately 95% use computers for administrative purposes. However, 2,000 or more of these Offices do not have the IT staff needed to support them, and the vast majority of these Offices either have no Internet access or only insecure and highly inefficient slow speed dialup access.

The continuing availability of increasingly powerful but less expensive

computers and the still-emerging expanded availability of high-speed Internet access, as well as other related technology developments, could all have a considerable impact on small and rural law enforcement agencies. Information sharing, remote site training, and improved communications across large jurisdictions, are examples of how technology could benefit small and underserved rural departments. Further, the falling costs of this technology put it within the reach of more small and rural departments than ever, especially if given Federal fiscal support.

The NSA Pegasus Program is designed to build upon these technology developments, as well as innovative uses of new technology, to bring a cohesive and responsive approach to local agency data interoperability, especially focusing on small and underserved rural areas. This approach is entirely supported by Federal studies showing that computer interoperability enhances the quality of justice.⁸

The Solution

The NSA Pegasus Program is needed because there is no other national program that addresses the lack of interoperable local law enforcement databases. Without support at the local level of the kind being advanced by the NSA Pegasus Program, local agency information sharing cannot occur to shore up everyday local law enforcement, or in support of the National response to the terrorist threat.

In FY02, the U.S. Congress authorized \$800,000 in funding for the National Sheriffs' Association (NSA), for

"The NSA Pegasus Program will continue its efforts to advance nationally-embraced automated data integration and data exchange standards, built on Federal policies, standards and guidance, driven by 'bottom-up' support."

***Dr. Lee Colwell
Executive Director
Pegasus Research Foundation***

development of a pilot system for multi-state information sharing of local law enforcement information. That funding made possible a pilot system with a limited purpose: to serve as a demonstration project that would identify problems and lessons learned in creating multi-state information sharing systems serving local agencies. In FY03, the Congress authorized an additional \$4,750,000 for initial deployment of the NSA Pegasus System.

In the Summer of 2002, the National Sheriffs' Association, with the support of NSA leaders and members, asked the Pegasus Research Foundation to conduct a focus group of the Nation's Sheriffs to analyze the problems and issues that create barriers, technological, institutional or political, involved in multi-state or interstate information sharing by local agencies. In addition, the NSA asked that a model approach be identified for ongoing governance, cost minimization through shared infrastructure, and funding of a multi-state information sharing system. The NSA mandate was to focus first on addressing the following generally stated multi-state local law enforcement information sharing needs:

- "Bottom-up," local agency driven, information technology solutions.
- Multi-state (or interstate) sharing of local information.
- Utilizing corporate quality emerging technologies, especially the Internet.

On November 9, 10 & 11, 2002, the NSA Pegasus Forum Focus Group was conducted in Orlando, Florida with participating Sheriffs representing a broad cross-section of the Nation's 3,088 Sheriffs: rural and urban; large and small; self-dispatching and mutually assisted dispatching offices. Representing such a broad spectrum of Sheriff's Offices, the participants presented unique insight into the problems and needs for information sharing as they, the Sheriff, lives it, not as others might theorize their needs. This insight was considered especially important for the rural Sheriff, a group that represents 84% of all Sheriffs. Of the 3,088 Sheriffs' Offices nationwide, 2,596 (or 84%) of these Offices serve populations of less than 100,000,⁹ while 2,207 Sheriffs' Offices (or 71% of the total) serve rural populations of less than 50,000.¹⁰ The following summarizes the deliberations of the Pegasus Forum Focus Group.

Sheriffs attending the Focus Group were first briefed on the problem and provided with a proposed vision for the establishment of a program to address the problem. They also were provided a proposed mission statement, goals, and an organizational and governance structure. The Sheriffs in attendance first confirmed that the problem of inadequate data interoperability is a significant nationwide problem and that the NSA Pegasus Program is the vehicle best suited for Sheriffs to address the problem. Participating Sheriffs acknowledged that information sharing depends on "data interoperability"—computers that "talk to each other"—and that Sheriffs' Office computers often do not "talk to each other." The Sheriffs concurred that, despite the national policy of information sharing, no other national program is dedicated to solving this lack of data interoperability.

With this consensus, the Sheriffs reviewed, discussed, and gave unanimous agreement to the following NSA Pegasus Program vision statement: "Through the NSA Pegasus Program, Sheriffs will exercise national leadership at the

county level, leading a fundamental reorientation for many in the Nation's local law enforcement community of viewing and using IT information sharing as a direct contributor to mission accomplishment by participating agencies nationwide."

Next, the Sheriffs came to concurrence on the following Pegasus Program Mission Statement: "It is the Mission of the NSA Pegasus Program to meet the problem of inadequate local law enforcement Data Interoperability, by:

Determining what is available to Sheriffs, and what computer systems Sheriffs need, to be able to access and manage information for information sharing, and

Assuring the availability to Sheriffs of the multi-state information sharing capabilities necessary to meet those needs."

With the vision and mission established, the Sheriffs next considered Pegasus Program goals. Following review and deliberation, the Pegasus Program's goals were established as follows:

"The objective will be to prove information in sheriffs' legacy systems can be made accessible to other users, and also across county and state lines, to solve a two-part national problem—computerized records in sheriffs' offices that cannot be electronically accessed, and sheriffs' offices that do not have the resources for the computerization of records and the broadband interconnections needed to share information."

***Sheriff Wm. T. (Tommy) Ferrell
Sheriff, Adams County, MS
Chairman, NSA Pegasus Advisory Board***

- “To enable the nation’s Sheriffs and other local agencies they work with to share information quickly, easily and appropriately—between and among local law enforcement; with first responders and public health; with State and Federal law enforcement; with private sector entities having critical infrastructure protection responsibilities; and with the public.
- To assist Sheriffs and other local law enforcement in securing and protecting information.
- To see that IT services provided as part of the Pegasus Program are reliable, secure, trusted and cost-effective.
- Ultimately, to enable local law enforcement to use IT and IT training to improve law enforcement effectiveness and performance.
- To assist Sheriffs in leading efforts to share local records and information nationwide.”

Finally, the Sheriffs reviewed and approved an Organization and Governance structure, the salient points of which include the following:

- “Sheriffs will identify other local agencies in their counties that they want to share information with, such as municipal law enforcement, fire, EMS and public health agencies.
- Each Sheriff will retain complete control over the information his/her Office shares, and who has access to specific data of his/her Office.
- Sheriffs, with the support of the NSA, will set the information sharing policies and standards that apply to Sheriffs’ Offices.
- The NSA will outsource the Pegasus Program information-sharing infrastructure.”

Based on the findings of this Focus Group, during the Summer of 2003, the NSA Pegasus Program deployed a Pilot System Project which demonstrated the consensus for and feasibility of multi-state or interstate information sharing by local agencies. This Pilot System linked four Sheriffs’ Offices in three States, and focused on building consensus for, and then technically demonstrating, local agency database interoperability. The Pilot System Project integrated local agency law enforcement records across multiple agency platforms, and demonstrated the consensus achieved among Sheriffs as to how they want to share information between and among themselves and others with whom they work, and the

technical feasibility of doing so, laying a solid for nationwide deployment of the NSA Pegasus System.

CONCLUSION

A solid foundation for the NSA Pegasus Program has been laid. The program is a nonfederal multi-state immediate information sharing system designed by and for local law enforcement, utilizing COTS technology. It is operated to meet U.S. Department of Justice approved NIST standards by the Pegasus Research Foundation, in coordination with and for the National Sheriffs’ Association (NSA). NSA Pegasus is the only local agency driven effort to integrate existing local agency legacy databases nationwide. To preclude duplication of effort, NSA Pegasus has been developed in coordination with related Federal Programs, especially LEO and RISS. As such, NSA Pegasus is a critical part of the Nation’s Plan for Homeland Security, to be implemented at the local level in every county in the Nation.




The DHS white paper entitled The National Strategy for Homeland Security acknowledges the crucial role of state and local governments, private institutions, and the American people in securing our homeland. It also recognizes that the Federal government needs to do a better job of utilizing the capabilities of state and local law enforcement to prevent terrorism by giving them access, where appropriate, to the information in our federal databases, and by utilizing state and local information at the Federal level.¹¹

The NSA Pegasus Program will focus on integrating existing local agency databases using the DOJ Justice XML Data Model and eXtensible Markup Language (XML) tags, making the data in those databases easy to access by all authorized users. The GAO has encouraged the Congress to require that OMB move quickly to require Federal agencies to use XML. If NSA were not to exercise leadership here, it is certainly foreseeable that systems now being deployed would later have to be retrofitted, at great expense, to accommodate standard XML tags. Thus, NSA’s efforts to advance the DOJ Justice XML Data Model for local law enforcement systems is an important part of the solution to the problem of inadequate data interoperability.

Recognizing the necessity of Federal support for many Sheriffs and communities that otherwise lack the resources to participate in the NSA Pegasus Program, involved agencies must also realize that the NSA Pegasus Program must be a partnership, with no one level of government having complete autonomous control or policy establishment over the system.

The FY04 Request

The NSA Pegasus Program requested \$10 Million in continuation funding for FY04. Language in the House Subcommittee Report, No. 108-221 (p. 39), expresses concern about “information sharing initiatives that are being developed independently, with no apparent plan to integrate them with other systems operated by Federal law enforce-

ment and with RISS and LEO.” With continued funding in FY04, the NSA Pegasus Program will begin to connect police agencies, fire departments, utilities and other governmental and private sector critical infrastructure organizations and insure that, where possible, it utilizes existing communications infrastructure and is compatible with LEO and RISS. 

1. Ibid.
2. Critical Foundations-Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection. October 1997.
3. The National Strategy for Homeland Security, White Paper published by the Department of Homeland Security, July 2002.
4. Ibid.
5. “Public Safety and the Interoperability Challenge,” by Brenna Smith; National Institute of Justice Journal; April 2000.
6. Statement of Mark A. Forman, Associate Director for Information Technology and Electronic Government, OMB before the Committee on Government Reform Subcommittee on Technology and Procurement Policy, U.S. House of Representatives, June 7, 2002.
7. Hart-Rudman Report “America Still Unprepared—America Still in Danger,” Council on Foreign Relations, November 2002.
8. “Crime and Policing in Rural and Small-Town America: An Overview of the Issues,” NIJ Research Report, September 1995; by Drs. Ralph A. Weisheit, L. Edward Wells and David N. Falcone.
9. Sheriffs' Offices 1999, Bureau of Justice Statistics, May 2001, NCJ 186479.
10. Ibid.
11. National Strategy for Homeland Security, White Paper published by the Department of Homeland Security, July, 2002.

Pegasus Research Foundation

National Sheriffs' Association (NSA) Pegasus Program


Meeting the information sharing needs of Sheriffs and those they work with

Integrated Databanks Cause Concern for Foreign Visitors

A massive effort is underway to integrate more than two dozen criminal and terrorist databanks as part of a new immigration tracking system. The Department of Homeland Security plans to integrate 27 different biographical databases and one biometric database this year to make the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program work. US-VISIT requires that most foreign visitors traveling to the U.S. on a visa have their two index fingers scanned and a digital photograph taken to verify their identity at the port of entry.

An issue of concern to some immigration advocates is the fact that inaccurate information may cause problems for people entering the country. Last March, the FBI announced that it was exempting databases within its National Crime

Information Center, Central Records System, and National Center for the Analysis of Violent Crime from compliance with accuracy regulations under the 1974 Privacy Act. While the FBI states it makes every effort to ensure accuracy, it says, “it is impossible to determine in advance what information is accurate, relevant, timely and complete.” Judith Golub, a representative from the American-Arab Anti-Discrimination Committee said visitors to the U.S. might find their information being compared with inaccurate FBI data, causing confusion and unnecessary detentions.

For more information visit the Department of Homeland Security at: www.dhs.gov/dhspublic/display?content=3043 or www.govexec.com/dailyfed/0104/010704c1.htm. 



Private Sector Responds to WA Call for Education

by Brian LeDuc

Brian LeDuc became Washington State's Justice Information Network Program Director in April 2003. Prior to accepting that position he served as counsel to the electronic public access program of the federal courts and as an American Bar Association liaison on a legal reform in Macedonia.

The January/February issue of *Integration News* discussed the formation of Washington State's Justice Information Network, the biggest challenges to implementing a statewide integration program, and six principles for making an effective start. In this update, Mr. LeDuc reports on the responses received to Washington's RFI and the current status of the project.

In October 2003, the Washington State Justice Information Network (JIN) Program Office issued a Request for Information (RFI). The RFI expressed the goal of understanding the nature and scope of what it might mean to develop an integration solution for the state—the task that the law has essentially assigned to the governance structure for JIN (the Integrated Justice Information Board).

When the RFI was issued, there was considerable skepticism as to what might result. It asked for assistance with some complex questions, as well as a proof-of-concept, to be delivered at no cost to the state. Compounding internal fears of the questionable desirability of filing a response, many of the subsequent technical questions asked about what kind of request for proposal (RFP) would follow. In answer, the Program Office had to admit that an RFP was not a certainty, and that it was dependent on securing funding—in a state already strapped for cash.

The proposals, all extremely well-prepared and brimming with both general and specific information, offered a variety of possible solutions, many of which were already working in other states or local jurisdictions. From data warehouses to enterprise service bus (ESB) technology, an array of choices and strategic directions were presented for review.

After meeting to discuss the proposals, the TAG agreed to invite four of the respondents to make presentations. For the most part, solutions that were judged as overly proprietary or more centralized in nature were seen as less desirable than more open, diffused models, which might help individual agencies or jurisdictions to work independently in a collaborative environment.

The presentations, which were held on February 3, were

“Solutions that were judged as overly proprietary or more centralized in nature were seen as less desirable than more open, diffused models, which might help individual agencies or jurisdictions to work independently in a collaborative environment.”

again, extremely well-done and informative. Of the four vendors, two, Equarius¹ (in partnership with Microsoft) and Online Business Systems² (in partnership with Sonic Software) were invited to collaborate on proof-of-concept projects for the state. Both of these companies are already doing significant integration work in the state (Equarius with King County, Online with the

city of Seattle), and both demonstrated expertise in both the current environment in Washington and the steps by which a statewide integration effort ought to proceed.

The Equarius proposed solution uses Microsoft Biz Talk server and XML-based technologies to share data between diverse systems. Their proof-of-concept development efforts, which are just getting underway at this time, propose to publish data from the State Patrol system as a web service, which will facilitate its exchange in a variety of ways with members of the justice community.


The Online system uses ESB technology to develop a suite of exchanges in an open architecture. Their proof-of-concept, which is also still in the planning phase, proposes an exchange of citation data among the Seattle Municipal Court, the Administrative Office of the Courts and the Department of Licensing.

Both of these projects offer an opportunity to demonstrate that the technology can work and that integration can be accomplished in a multifaceted environment with minimal

“Both of these projects offer an opportunity to demonstrate that the technology can work and that integration can be accomplished in a multifaceted environment with minimal impact on existing systems.”

While the arrival of the first response on December 19 allayed fears that no company would be interested, the arrival of the eighth response created new fears that the Technical Advisory Group (TAG) might be overwhelmed by the mountain of information that now needed to be reviewed.

impact on existing systems. The viability of each and the willingness of the state to embrace and fund a collective solution, still remain to be seen. Nevertheless, the JIN has taken an important step toward turning its vision of improving public safety by providing criminal justice practitioners with complete, timely and accurate information, and improving operating efficiency by facilitating the integration of disparate systems throughout the state into a reality. And it has done so thus far at no cost to the state.

You can follow the progress of these efforts at www.jin.wa.gov. 

1. www.equarius.com.
2. www.online-usa.com.




Maryland Counties Create Integrated Network

Several departments in four Maryland counties have created a shared information system built on real-time access to local, state, and federal crime databases over a wireless network called Info-Cop. This is the first time agencies in Wicomico, Dorchester, Worcester, and Somerset Counties have been able to exchange real-time information between departments.

Spanning several Maryland counties, the Info-Cop system is rooted in Wicomico County's Salisbury Police Department. For seven years, the Salisbury PD has been using grant funding from the Local Law Enforcement Block Grant to invest in technology, with a focus on mobile data. This mobile data technology initiative has resulted in the department's development and management of the only mobile data switch on the Eastern Shore to utilize a public cellular network.

"Our intent in building the wireless network in Salisbury was to expand to our neighboring communities once it was operational," said Chief Allan J. Webster of the Salisbury Police Department. He also said today they are able to, "communicate over a much larger geographical area, while providing data-sharing and rapid-access information tools that were never before available to us."

The Salisbury network now has the ability to make a seamless connection to any potential partner department using any heterogeneous network including CPDP, GRPS, IX, and CDMA, as well as private radio. Maryland's network is expected to increase later this year to include seven counties and a total of 21 agencies covering 3,337 miles and a population of 408,300. 

SUBSCRIBE NOW TO TAKE ADVANTAGE OF OUR PROMOTIONAL RATE!

Connecticut to Improve Officer Access to Information

Connecticut recently moved to begin modification of the Connecticut On-Line Law Enforcement Communications Teleprocessing (COLLECT) Revision Project, in support of the State's Department of Public Safety, Division of State Police.

COLLECT is the law enforcement officer's link to public safety information including warrants, protection orders, motor vehicle registrations, operator history, stolen property, criminal history, and offender status information. This information is critical to officers, front-line criminal justice personnel, and general public safety in a developing criminal incident or traffic stop. On-the-street officers, dispatchers, and criminal investigators are dependent upon its around-the-clock operation.

Under a newly signed contract, MAXIMUS will replace the current COLLECT system with a combination of commercially available, off-the-shelf products and custom products based upon public safety and open systems standards and architecture. This will provide over 13,000 authorized state, federal, and local police and criminal justice users access to state and national law enforcement information.

A partner in the project, Advanced Technology Systems (ATS), provides a web browser and message switch that will

be customized to support Connecticut's specific requirements and interfaced with Peak Performance Solutions nexTEST NCIC and State Certification web-based testing software. MAXIMUS will design, build, and integrate a supporting Oracle application and database with the ATS products and Connecticut's existing legacy information systems. COLLECT will be the State's single information conduit to national law enforcement systems, notably the National Crime Information Center (NCIC) and the National Law Enforcement Telecommunications System (NLETS).

The Connecticut COLLECT Revision Project will be among the first systems in the nation to implement the latest law enforcement national standards including NLETS XML messaging and rap sheets. As all states update their law enforcement message switching systems, they will adopt the same web-based technologies and XML justice standards used in COLLECT to satisfy increasing demands for public safety and justice integration. Systems such as COLLECT, that provide connections to nationally linked law enforcement systems, will play a significant role in homeland security initiatives and communications within the state and federal jurisdictions.

For more information visit www.maximus.com. 


Case Study *... continued from page 11*

Network-Centric Approach Leveraging Web Services

A network-based approach allows access to information on-demand. Information is retrieved, viewed, and only the required elements are presented to the receiving application—information isn't stored in a separate database or data warehouse. This dramatically reduces complexity, costs, and security exposures as information exchanges are built. Web services are software components delivered over the Internet using standardized technologies. SOAP is the core standard for Web services and defines a uniform way of passing XML-encoded data. It allows remote procedure calls using HTTP (Hypertext Transfer Protocol), allowing communication via the Internet between remote systems. The Internet is the physical network infrastructure, and SOAP is used to communicate XML messages via HTTP. A network-based integration approach using XML allows agencies to use existing applications and data sources, without adding a repository, servers, or building custom application interfaces. Standards like JusticeXML and LegalXML provide a common vocabulary and vendor-neutral environment.

Alaska's advice for other states going down the integration road:

- Document exchanges, so that you understand: Rules and statutes governing information sharing, business rules, triggers, timing, and source and target reconciliation.
- Don't get bogged down in modeling: Test it on an actual exchange, and implement exchanges as you model them.
- Get detailed information from experts and practitioners: Build a dedicated, cohesive group committed to resolving issues.
- Have the authority to make decisions: Write a clear charter signed by all agencies.

The entire MAJIC team is justifiably proud of its accomplishment, and looks forward to the next successful exchange. XAware, Inc. is proud and happy to be part of Alaska's success. 

Conferences and Events

Roadmap for Information Sharing:

A Seminar for Justice Information Systems Decision Makers and Managers

April 6-8, Baltimore, MD; May 4-6, Chicago, IL; May 18-20, Phoenix, AZ; June 9-11, Atlanta, GA.

The National Criminal Justice Association in cooperation with the IJIS Institute and the Justice Information Sharing Professionals (JISP) is presenting a series of regional seminars exploring useful aspects of a framework for justice information sharing. Topics covered in the seminar include: governance, security, privacy, measuring project success as well as technology choices along the way. These seminars are designed to help managers who are or may become involved in implementing information sharing technology among law enforcement and criminal justice organizations to increase the effectiveness of justice processes and provide greater homeland security. There is no registration fee, but participants are responsible for all costs incurred to attend the seminar. For more information: www.ncja.org.

NCSC's Planning, Acquiring, and Implementing Court Technology

April 26-28, 2004, Williamsburg, VA.

Discover how to develop an effective technology budget request, use the National Model RFP, and understand and better negotiate technology purchase and maintenance contracts. Court managers must have an understanding of how to acquire, implement, and manage court technology effectively. For more information: <https://secure.ncsc.dni.us/icm/reg.html>.

Government Technology Conference (GTC)

May 10-14, 2004, Sacramento, CA.

GTC features nationally known speakers, dozens of relevant workshops and seminars and exhibits from hundreds of computer and telecommunications firms featuring information technology solutions for state and local government. For more information: www.govtech.net.

Developer's Workshop: Global Justice XML Data Model

May 11-13, 2004, Atlanta, GA.

The U.S. Department of Justice, Office of Justice Programs (OJP) is pleased to offer the first public training workshop on GJXDM version 3.0. This workshop is specifically designed for developers and practitioners in the field to provide the information needed to bring them up to speed on the newly released 3.0 version. This workshop will be a highly technical session and will include: hands on exercises, experienced presenters, and actual case studies.

Registration information will be available in March at <http://it.ojp.gov/GJXDMregister> or visit: www.ncja.org/pdf/GJXDM_Developers_Workshop.pdf.

International Conference on Biometric Authentication

July 15-17, 2004, Hong Kong.

The purpose of this conference is to emphasize the design and development of efficient and effective biometric technologies and systems, provide an international forum for researchers, engineers and vendors from different disciplines to exchange ideas, identify problems, evaluate system performance, explore new research directions, and initiate possible collaborative research and future system developments. This conference will significantly benefit biometric researchers in academic, government, and industrial sectors. For more information: www4.comp.polyu.edu.hk/~icba/.

From Prison to Home: Supporting Communities, Families, and Inmates National Criminal Justice Association National Forum 2004.

August 7-11, 2004, Chicago, IL.

Save the dates for this outstanding upcoming conference. Details soon to come.

For more information: www.ncja.org/pdf/savethedates.pdf.



BGL Publishing
P.O. Box 68
Milbank, SD 57252

IntegrationNews

CRIMINAL JUSTICE DATA INTEGRATION



IntegrationNews

CRIMINAL JUSTICE DATA INTEGRATION

BGL Publishing
P.O. Box 68
Milbank, SD 57252
(605) 432-6801

Special Promotional Offer \$95!

Five Convenient Ways to Subscribe:

E-mail: subscribe@integrationnews.com • **Website:** www.integrationnews.com
Phone: (605) 432-6801 • **Fax:** (605) 432-9121 • **OR Mail** this form with check to:
Integration News • P.O. Box 68 • Milbank, SD 57252

**Promotional
Code 42-A**

Name _____ Title _____

Agency/Company _____

Street Address _____ City/State/Zip _____

E-Mail _____ Phone: _____ ☐ Please send me an invoice.

Promotional Price (Code 42-A)

- ☐ One year (6 issues) Electronic Copy \$95
- ☐ One year (6 issues) Hard Copy \$95

Regular Price

- ☐ One year (6 issues) Electronic Copy \$125
- ☐ One year (6 issues) Hard Copy \$149

* Feel free to copy and distribute your subscription issues throughout your agency or company.