

Law Enforcement Information Sharing and the Implications for Local Government (A Technical Reference)



Law Enforcement Information Sharing and the Implications for Local Government (A Technical Reference)

Introduction

“We are all on the same team” is a phrase used often in law enforcement, especially when it becomes necessary to remind everyone that the

Advances in information and communication technology (ICT) have created amazing opportunities for law enforcement professionals at local, state

To take advantage of the opportunities these tools create, criminal justice agencies have formed multi-jurisdictional and regional relationships designed to combine, cross-match and share data from a wide variety of sources. Until now the U.S. Department of Justice has supported these collaborative efforts through a series of ‘pilot’ project grants. These pilot projects have been successful in that they have shown the utility of collaboration and information sharing. However, it is time now to shift from pilot projects to more effective implementations based upon lessons learned.

In today’s environment, successful law enforcement requires more than just a willingness to work together. It requires the ability to effectively share data, information and intelligence across multiple jurisdictional boundaries in a secure and efficient manner.

distinctions and rivalries that come with differing uniforms must not be allowed to distract from the common goal of protection and enforcement. In today’s environment, successful law enforcement requires more than just a willingness to work together. It requires the ability to effectively share data, information and intelligence across multiple jurisdictional boundaries in a secure and efficient manner.

and federal levels to collect, categorize, cross-reference and share data and intelligence in a way that often results in a wealth of actionable knowledge.

In 2006, the [Justice Research and Statistics Association](#) conducted a [survey](#) of information-sharing initiatives either in existence at that time or under development in the states. While they were

“Leading jurisdictions across the country have a mobility infrastructure woven into the fabric of the agency, providing the law enforcement community with the tools and intelligence needed for better, faster decision-making,” says Digital Communities Law Enforcement Information Technology Task Force (LEITTF) industry member Pat Thetford from AT&T.



not completely satisfied with their survey response rate, they were able to identify 266 information-sharing systems in place in 35 states and Canada.

As one public sector LEITTF member recently commented, “There is a scream-

ing need for a review of all the regional law enforcement information-sharing systems floating around out there. I hate to see us continue to fund additional pilot/grant projects without any goal of finding one or two systems that will meet most of

our needs.”

This is the time for federal, state and local agencies to increase their efforts to work together and build upon a common standards-based infrastructure rather than continue the development of separate systems.

Mapping the Way Ahead

The LEITTF members believe that a case has been made for multi-jurisdictional information sharing and that the fundamental building blocks of data and technical interoperability standards are now in place. What is needed is for local government to better understand what already exists so that it can be leveraged in all future plans and acquisitions. Thereby creating a platform for sharing that can be easily built upon and expanded over time.

Law enforcement ICT needs must be considered and addressed as cities, towns and counties strive to consolidate their IT infrastructures. Unfortunately, much of the good work done over the past several years in criminal justice information sharing has resulted in confusing sets of systems, standards and organizational contributions.

To that end, the LEITTF is constructing a technical reference containing overview information from just a few of the most common and widely accepted standards, systems, programs and organizations available to support local officials as they seek to improve their information-sharing capabilities.



For some, this guide may be a review, but for others it may serve as an introduction to the law enforcement technology and information-sharing community. Hopes are that it will prove to be at least a reasonable catalyst for long-serving law enforcement professionals, newly assigned enterprise IT support staff, and private sector providers

of law enforcement information tools and services to engage in the important conversations necessary to fully understand the needs and opportunities now facing the local law enforcement community.

A Long-Standing Issue

There is one issue that has perhaps challenged and frustrated proponents of multi-jurisdictional law enforcement information sharing more than any other: information ownership and control.

change to this way of thinking. The report focuses primarily on federal agencies, but there are lessons included in the analysis for law enforcement agencies at every level.

War assumptions are no longer appropriate. The culture of agencies feeling they own the information they gathered at taxpayer expense must be replaced by a culture in which the agencies instead feel they have a duty to the information to repay the taxpayer's investment by making that information available."

"The culture of agencies feeling they own the information they gathered at taxpayer expense must be replaced by a culture in which the agencies instead feel they have a duty to the information to repay the taxpayer's investment by making that information available."

– 9-1-1 Commission Report

Traditionally, law enforcement intelligence sharing has been conducted in a task force environment where there was an immediate and tactical need for information. Within those narrow confines, multiple agencies were able to establish trust relationships. Today, advances in information technology allow virtually anyone to view and share data. This fundamental shift is disconcerting for many since they are no longer able to control access to data as they did in the past. One of the most common and wide-spread controls has been the requirement that participants demonstrate a "need to know" before they are provided with information.

In the aftermath of the Sept. 11 terrorist attacks, the 9-1-1 Commission issued a [report](#) calling for a fundamental

The Commission stated the problem this way: "What all these systems have in common is a system that requires a demonstrated 'need to know' before sharing. This approach assumes it is possible to know in advance who will need to use the information. Such a system implicitly assumes that the risk of inadvertent disclosure outweighs the benefits of wider sharing. Those Cold

Excessive information compartmentalization in the name of security serves no one well. Modern systems and processes enable authorities to establish accountability and oversight capabilities to ensure that access and use comply with policy and law. Real-time tracking and auditing of system users and their activities guarantees that they do so in a manner consistent with their mission, authorities and responsibilities. A more robust implementation of available tools can do much to help rebalance the historical equation and make the rewards for sharing greater than the risk of inadvertent disclosure, thereby improving overall intelligence sharing and law enforcement success.



National Standards

LEITTF member [Paul Wormeli](#), executive director of the [Integrated Justice Information Systems \(IJIS\) Institute](#), captures the consensus view of LEITTF when he describes the benefits of standards this way: “Standards make the most sense when we deal with the information exchanges, not the underlying individual systems. Particularly with a services-oriented architecture, it is the exchange that needs to build on open standards.”

National Information Exchange Model (NIEM)

Perhaps the most widely recognized and important standard of the day is the [National Information Exchange Model \(NIEM\)](#). NIEM is a partnership between the [U.S. Departments of Justice \(DOJ\)](#) and [Homeland Security \(DHS\)](#), and enables information sharing — focusing on information exchanged among organizations as part of their current or intended business practices.

NIEM addresses cross-domain information exchange activities. When combined with a supporting architecture and implemented with Web services, the cost of system development is minimized and the time to deliver is significantly reduced.

NIEM is seen by many in the justice information-sharing community as the key standard and foundation for exchanging information across multiple domains and disciplines. Because of this, all grants from the DOJ or DHS now carry special conditions requiring that information systems

Perhaps the most widely recognized and important standard of the day is the National Information Exchange Model (NIEM). ...NIEM is seen by many in the justice information-sharing community as the key standard and foundation for exchanging information across multiple domains and disciplines.

that share data must conform to NIEM specifications and guidelines to better promote increased information sharing. Grantees agree to make all schemas generated as a result of their grant available through the component registries.

State and local governments are traditionally skeptical when it comes to the federal imposition of standards. However, NIEM standards are generally viewed as reasonable and helpful. LEITTF member Peter Gnas, network manager with the Milwaukee Police Department, describes them this way: “...a good example of a broad-based framework which outlines how each agency can package their data in a universally acceptable method.”

The graph on page 6 demonstrates [NIEM-based developments and implementations](#) across the country as of October 2009.

Global Justice XML (Global JXDM)

The [Global Justice Extensible Markup Language \(XML\) Data Model \(Global JXDM\)](#) is an XML standard designed specifically for criminal justice information exchanges

that provides law enforcement, public safety agencies, prosecutors, public defenders and the judicial branch with a tool to effectively share data and information in a timely manner.

The Global JXDM removes the burden from agencies to independently create exchange standards, and because of its extensibility, there is more flexibility to deal with unique agency requirements and changes.

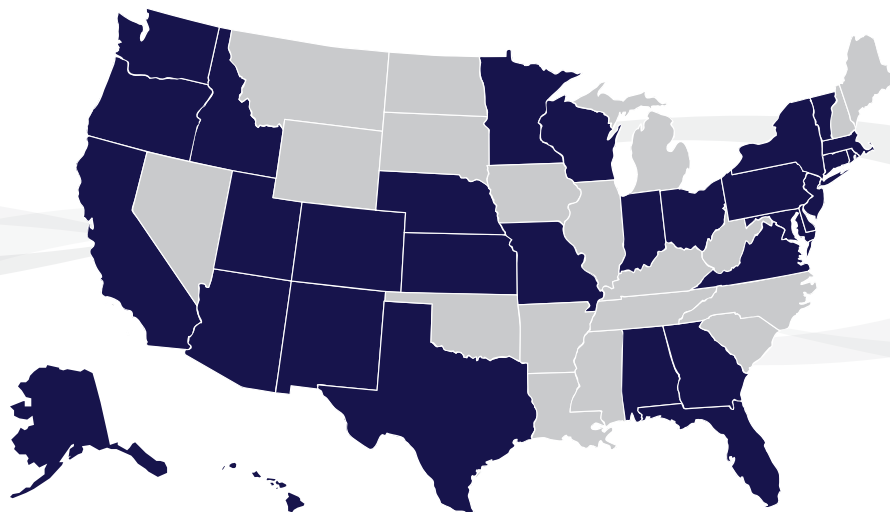
The Global JXDM is sponsored by the [U.S. Department of Justice \(DOJ\) Office of Justice Programs \(OJP\)](#), with development supported by the Global Justice Information Sharing Initiative’s (Global) XML Structure Task Force (GXSTF).

U.S. DOJ Law Enforcement Information Sharing Program (LEISP)

Today, the most widely used NIEM-conformant exchanges include several based on the [Law Enforcement Information Sharing Program \(LEISP\) Logical Entity eXchange Specifications \(LEXS\)](#). LEXS is

NIEM-Based Developments and Implementations – October 2009

■ NIEM Implementation
■ Unknown



a family of IEPDs (Information Exchange Package Development) that defines a common format in which information can be shared and implements NIEM for many common types of law enforcement information exchanges. LEXS specifies how law enforcement information should be packaged and delivered to information-sharing applications and how partnering applications can implement federated search capabilities. The most commonly used elements form the foundation upon which practitioners can build specialized extensions to suit individual communities.

Global Justice Information Sharing Initiative (Global) Justice Reference Architecture (JRA)

The Global JRA (Global) specification is intended to be a technical implementation architecture that addresses the full

range of information-sharing use cases, and provides a comprehensive blueprint for implementing interoperable data sharing services and capabilities. Global supports the view that this dynamic interoperability strategy will help to prevent incompatibilities, guide vendors and organizations on how to fit components together, and facilitate communication and interoperability between disparate communities.

Justice Information Exchange Model (JIEM)

The Justice Information Exchange Model was developed by SEARCH through funding from the U.S. Department of Justice, Bureau of Justice Assistance, to help jurisdictions across the country document their business information-sharing requirements and facilitate integrated justice information systems planning and

implementation throughout the nation.

SEARCH is a nonprofit membership organization created by and for the states. Its primary objective is to provide assistance in identifying and solving the information management problems of state and local justice agencies confronted with the need to exchange information with other local agencies, state agencies, agencies in other states, or with the federal government electronically at key decision points throughout the justice process. Through identification of these key decision points, and the information that flows between various justice entities at these critical exchange points, state and local practitioners are provided with an enterprise-wide view of information-sharing priorities.

National Systems Overview

Television crime shows like CSI, NCIS, Law and Order and many others are a very visible component of popular culture and have often set an expectation with the viewing public that law enforcement professionals have an instantaneous ability to access intelligence data from around the world and across every aspect of the economy. Of course, the reality for local law enforcement is often much different than what is portrayed on television. However, there are some national systems already in place that can and do support local law enforcement efforts. Consequently, their capabilities and limitations must be at least generally understood by all those responsible for supporting criminal justice information sharing within local communities.

Law Enforcement National Data Exchange (N-DEX)

The Federal Bureau of Investigation (FBI) has initiated the National Data Exchange (N-DEX) to provide law enforcement agencies the ability to share crime information on a national scale. N-DEX provides agencies the ability to search, link, analyze and share criminal justice information such as incident/case reports, jail data and parole/probation data from across the nation. N-DEX offers investigative, tactical and strategic benefits through nationwide searches from a single access point and detects relationships between and among people, vehicle/property, locations and/or crime characteristics. It connects the dots between data that is not seemingly related.



N-DEX's initial focus is on large agencies and aggregated data sources, such as Regional Intelligence Centers (RICs), but will expand to any law enforcement agency.

FBI's Regional Data Exchange (R-DEX)

R-DEX provides an interface to RICs to enable the search for unstructured documents and to retrieve matching documents. R-DEX serves two main functions: providing RICs with access to the U.S. Department of Justice's (DOJ) data and enabling a RIC user to perform full-text searches over DOJ unstructured documents for the region, in addition to the state and local documents accessed internally.

Federal Bureau of Investigation's (FBI) Law Enforcement Online (LEO) System

LEO is a national, interactive computer communications system and information intranet exclusively for the law enforcement community. The LEO system is a sensitive

— but unclassified — real-time, information-sharing communications system for all levels of the law enforcement community and is available at no cost to its users. LEO provides secure e-mail capability, a national alert mechanism and access to over 125 special interest groups for sharing information by providing access to other networks, systems, databases and other services.

National Law Enforcement Telecommunications System (NLETS)

NLETS is a 501(c)(3) not-for-profit organization owned and governed by the states that provides an international, secure, computer-based message switching system that links together state, local and federal law enforcement and justice agencies for the purpose of information exchange. It provides information services support for a growing number of justice-related applications with nearly 90 million messages transacted each month.

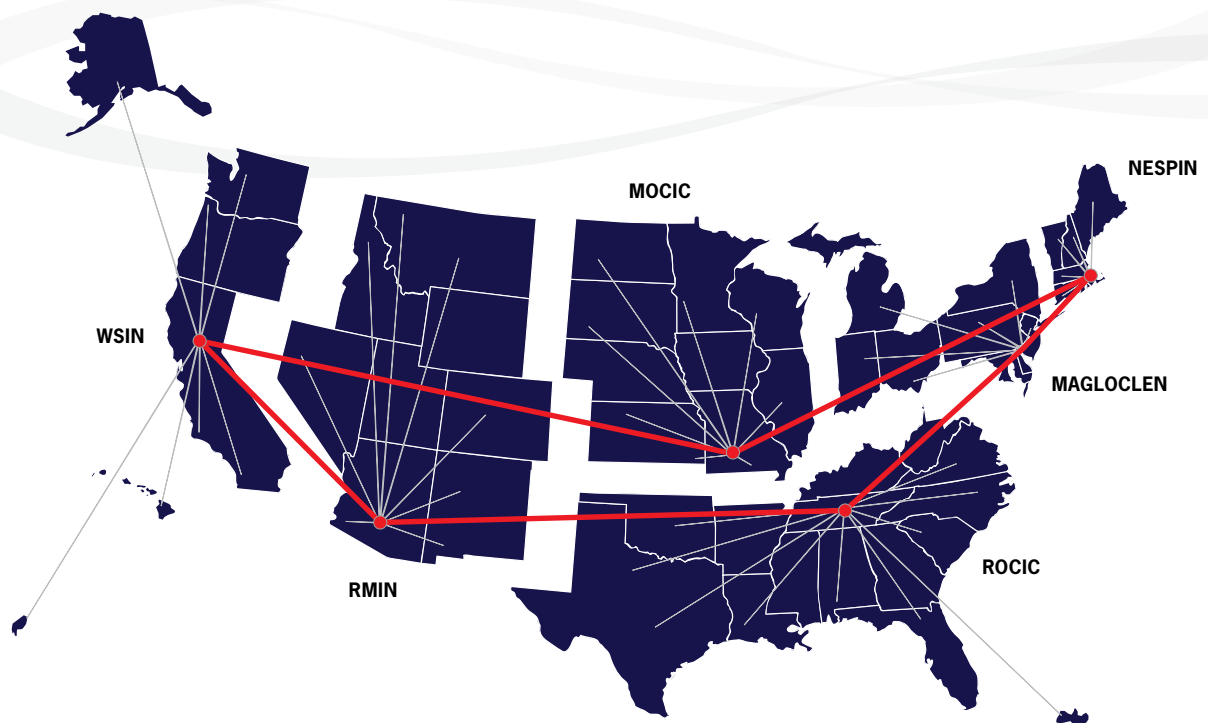
Regional Information Sharing System (RISS)

RISS is a national program of regionally-oriented services designed to enhance the ability of local, state, federal and tribal criminal justice agencies to:

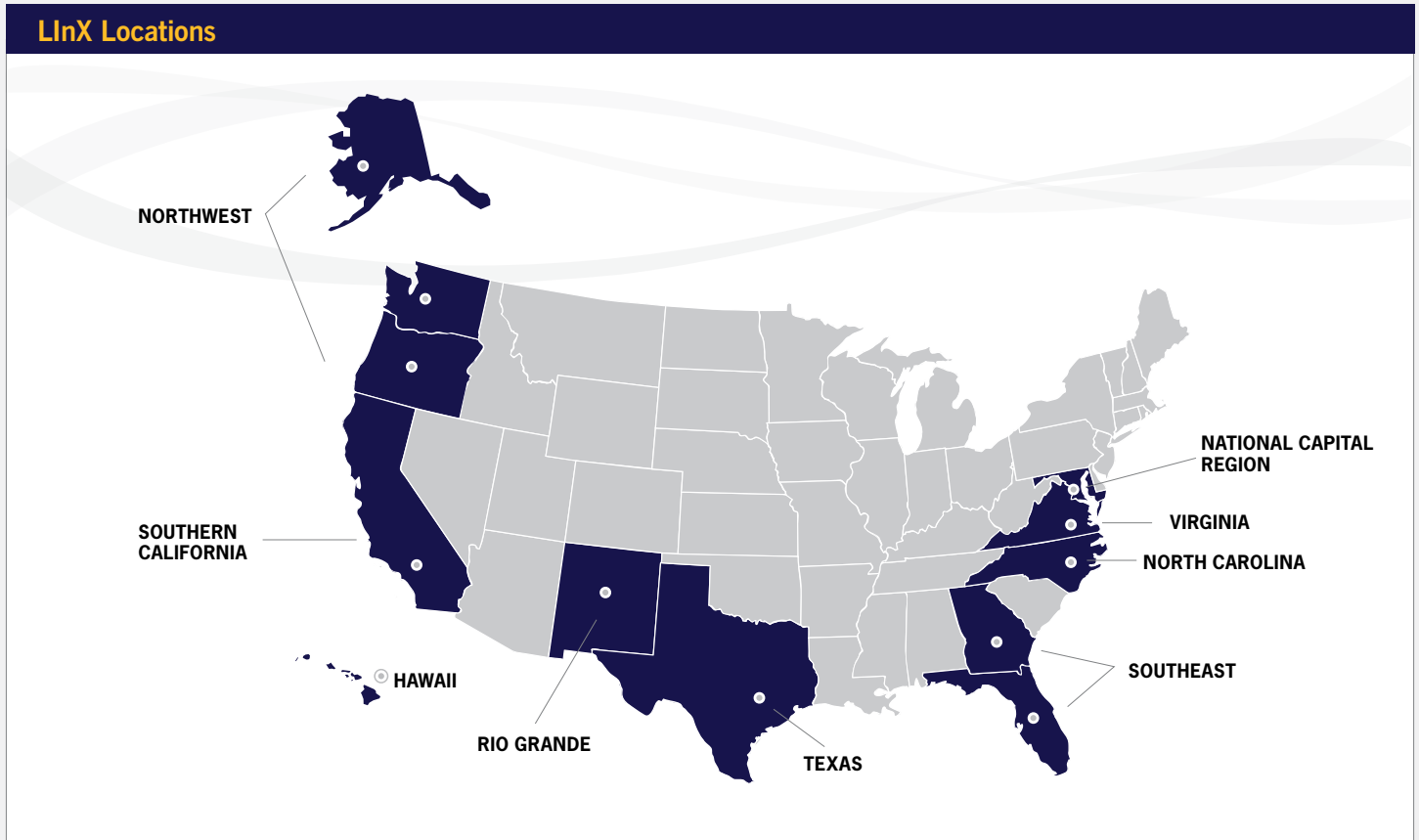
- identify, target and remove criminal conspiracies and activities spanning multi-jurisdictional, multi-state and sometimes international boundaries;
- facilitate rapid exchange and sharing of information among the agencies pertaining to known suspected criminals or criminal activity; and
- enhance coordination and communication among agencies that are in pursuit of criminal conspiracies determined to be inter-jurisdictional in nature.

The RISS Program operates in all 50 states, the District of Columbia, U.S. territories, Australia, Canada and England. RISS is the collective effort of six regional centers. While the RISS Centers operate independently and are tailored to support the unique needs of the region served, they also operate as a collective body to address national criminal justice issues.

RISS Centers



Regional Systems



While a single, fully integrated national system able to provide information to every law enforcement agency in the nation may be the absolute ideal, the reality is that significant progress has been made through bringing regional partners together in voluntary collaboration.

There are many examples of regional collaboration — some may say too many examples. However, the reality is it is through these partnerships that the best progress is being made and the necessary lessons learned that may one day carry us to the point where a fully integrated

national system is feasible.

The following systems are offered as examples of what is possible when regional partners purposefully decide to work together. They are comprised of differing technologies and differing management and governance structures, but they all demonstrate an improvement in law enforcement information sharing that stretches from the data center to the officer on the street.

LInX

The Law Enforcement Information Exchange (LInX) is an award-winning system

that was initially launched by the Naval Criminal Investigative Service (NCIS) — the felony investigative arm of the Department of the Navy (DON) — as a project designed to enhance information sharing between local, state and federal law enforcement in areas of strategic importance to the DON. LInX provides participating law enforcement agencies with secure access to regional crime and incident data and the tools needed to process it, enabling investigators to search across jurisdictional boundaries to help solve crimes and resolve suspicious events.

The LInX system is a regionally cen-



tralized data warehouse in which each agency participating in the system contributes information to the warehouse. The data contributed to the LInX system includes incident reports, case records, computer-aided dispatch events, citations, mug shots, pawn data and free text investigative documents.

According to Mark Calhoon, Newport News, Va., Police Department planning administrator, “LInX has grown to include 104 member agencies in Virginia including NCIS, the FBI, the U.S. Marshall’s Service, the Virginia Port Authority, the Virginia Department of Alcoholic Beverage Control and the Virginia State Police. In addition, there are similar LInX networks in: Alaska, Idaho, Oregon, and Washington (250 agencies); Texas (24 agencies); Georgia and Florida (58 agencies); New Mexico (23 agencies); Hawaii (six agencies); and the National Capital Region (80 agencies).” Calhoon believes that “LInX is a big initiative that deserves to get bigger.”

ARJIS

The Automated Regional Justice Information System (ARJIS) was created as a joint powers agency (JPA) to share information among justice agencies throughout San Diego and Imperial Counties, Calif. ARJIS has evolved into a complex criminal justice enterprise network used by 71 local, state and federal agencies in the two California counties that border Mexico. The secure ARJISnet intranet integrates more than 6,000 workstations throughout the 4,265 square miles of San Diego County. There are more than 11,000 authorized users generating more than 35,000 transactions daily.

OLLEISN

The Ohio Local Law Enforcement Information-Sharing Network (OLLEISN) is a system for sharing information among local law enforcement in Ohio. The OLLEISN mission is to create a voluntary Ohio local law enforcement information-sharing network, based on model policies

and established technical and security standards. Its purpose is to assist officers and investigators in preventing and responding to acts of terrorism and crime. Over 725 of the 900 local law enforcement agencies in Ohio share record management system (RMS) data through OLLEISN and have the ability to conduct in-depth searches and create reports based on subjects, persons, organizations, vehicles, property, report identifiers or locations.

The OLLEISN Tracking All Crime Known to Law Enforcement (TACKLE) system is a portable OLLEISN data mining type search tool enabling local law enforcement users to access in-depth search results and quickly research and categorize information. This information could include: interview notes; suspect, victim or witness information; property types; search warrants; pawn shop transactions; service

OLLEISN Guiding Principles are as follows:

- Maintain Local Law Enforcement Control
- Have Voluntary Participation of Agencies
- Require Agencies to “Give to Receive”
- Use State Standards
- Use National and Industry Standard Protocols and Open Systems Technology
- Use Security Standards and Best Business Practices
- Be *Provider Agnostic*
- Use a Scalable Environment

calls; registered offenders; concealed carry permits and firearm registrations; evidence; mug shots; finger prints and signatures.

Colorado COPLINK Implementation

In 2008, the public safety agencies in the Denver Metropolitan Area joined together and implemented Knowledge Computing Corporation's Coplink as their preferred multi-jurisdictional shared information system. Participating agencies defined a need for a secure, intuitive and easy-to-use and maintain system for querying across databases. They wanted a system that provided up-to-date data and had the tools to assist investigators in reporting, analyzing and graphically displaying links, associations, relationships and involvements in a practical and revealing manner. Additionally, they wanted a tool that would notify investigators of new or updated data relevant to their inquiries while protecting participating agency databases from intrusion, damage or being overly taxed by outside querying or repeated downloads. Agencies contributing data or allowing use of their data also needed to have the ability to limit access to only that data which they are willing to share.

The initial implementation in Jefferson County has now been expanded into other areas of the state with the Colorado Information Sharing Consortium (CISC) acting as the governing board for a statewide initiative to make the Coplink system available to law enforcement agencies throughout the state.

The CISC is comprised of seven public safety "core partners," including the Adams County Sheriff's Office, Arapahoe County Sheriff's Office, Aurora Police Department, Colorado Bureau of Investigation



Over 725 of the 900 local law enforcement agencies in Ohio share record management system (RMS) data through OLLEISN and have the ability to conduct in-depth searches and create reports based on subjects, persons, organizations, vehicles, property, report identifiers or locations.

(a branch of the Colorado Department of Public Safety), Denver Police Department, Douglas County Sheriff's Office and the Grand Junction Police Department.

Missouri Law Enforcement Data Exchange (Mo-DEx)

Mo-DEx is a statewide data warehouse also based on the Coplink solution suite. It conforms to the NIEM standard and interfaces with N-DEx. Mo-DEx provides law enforcement agencies with the ability to search, link, analyze and share criminal justice information such as incident/case reports; incarceration data; computer-aided

dispatch; photos; citations; collisions and pawn data on a statewide basis.

Mo-DEx was developed in cooperation with the Missouri Department of Public Safety, the Missouri Police Chiefs Association, the Missouri Sheriffs' Association, the Missouri State Highway Patrol, the Missouri Department of Corrections and the Office of State Courts Administrator. It was funded through a state and local law enforcement partnership which pooled federal funding to maximize the initiative's reach, effectiveness and return on investment.

Justice Information-Sharing Organizations

Efforts by federal, state and local law enforcement organizations and their private sector partners to improve justice information sharing are on-going and greatly enhanced by the work accomplished in justice information-sharing organizations. The following list of organizations represents some of the most respected, collaborative and long-standing activities. Most career law enforcement and communications professionals are well acquainted with these organizations, but as many communities move to consolidate their information and communications technology support activities people who have not historically supported law enforcement systems and activities are coming to positions of responsibility. The time is right for the efforts and products of these organizations to be shared with a broader audience within the local government technology community.

IJIS Institute

The IJIS Institute is the only national organization that brings together industry and government in an effort to improve national security and promote effective information sharing across all levels of the justice, public safety and homeland security communities.

International Association of Chiefs of Police (IACP)

IACP is a nonprofit membership organization of police executives working to advance professional police services;

promote enhanced administrative, technical and operational police practices; and foster cooperation and the exchange of information and experience among police leaders and police organizations.

Association of Public-Safety Communications Officials International (APCO)

APCO is a member-driven association of communications professionals that provides leadership, influences public safety communications decisions of government and industry, promotes professional development and fosters the development and use of technology for the benefit of the public.

Justice Information Sharing Practitioners Network (JISP)

JISP is a national network of state and local justice and public safety practitioners interested in best practices, standards and resources for solving the issues of infor-

mation sharing within the criminal justice community at local, state, regional and national levels.

National Association for Justice Information Systems (NAJIS)

NAJIS is an organization of individuals who are responsible for the acquisition, operation and management of local, state and federal criminal justice information systems.

Institute for Intergovernmental Research (IIR)

IIR is a nonprofit research and training organization specializing in law enforcement, juvenile justice, criminal justice and homeland security issues. Through the Global Infrastructure/Standards Working Group (GISWG), IIR supports the development of a conceptual framework that supports national justice information sharing and identifies strategies and tactics that will implement that framework.



Conclusion: Three Things You Can Do Now

...this can be the perfect time to change the often rigid and parochial structure of law enforcement information management, create new relationships and develop new collaboration and information-sharing methods and protocols.

Here are a few things you can do now to improve your agency's information-sharing capability. Even starting small by simply looking to share information that is easy to share with those agencies and jurisdictions closest to you will help establish a culture of openness and collaboration that will make it easier to move on to larger, more complex relationships in the future.

1. Make an organizational commitment to create a culture and structure for sharing information however and whenever possible with other departments and agencies. Great success can come if you are willing to adopt a "share unless there is good reason not to" approach instead of a "share only under special circumstances" policy. There are guidelines in the [*National Criminal Intelligence Sharing Plan*](#) to help you.
2. Become a member of the FBI's Law Enforcement Online (LEO) system. LEO is available at no cost to its users and provides secure e-mail capability; a national alert mechanism; and access to special interest groups for sharing information by providing

access to other networks, systems, databases and other services.

3. Take full advantage of the Internet, law enforcement Web sites and information-sharing opportunities like those highlighted in this report created by local, state and federal organizations. The Internet provides a wealth of open-source information, including government information and access to private agencies that share with law enforcement. Information-sharing and collaboration opportunities are available through sites like the [*Digital Communities Law Enforcement Information Technology Task Force*](#). Also available are national plans and reports outlining strategies for improved information sharing such as the following: the [*BJA National Criminal Intelligence Sharing Plan*](#), [*The Markle Foundation Task Force on National Security in the Information Age*](#), the [*DOJ IT Strategic Plan Fiscal Years 2008-2013*](#) and the [*Law Enforcement Information Sharing Program \(LEISP\)*](#).

There is both a need and an opportunity for local law enforcement agencies to improve their information-sharing capabilities. Both must be evaluated in the harsh context of the current financial situation in which most local governments find themselves. It is a very difficult time to begin something new if it requires any additional funding. However, this can be the perfect time to change the often rigid and parochial structure of law enforcement information management, create new relationships and develop new collaboration and information-sharing methods and protocols. Such changes don't require a large amount of cash but rather a full measure of vision and courage; something law enforcement officials traditionally have plenty of, regardless of economic cycles.

The Center for Digital Government and *Emergency Management* would like to thank the *Digital Communities* Law Enforcement Information Technology Task Force members for their support and assistance in the creation of this report with special recognition to the following task force members for their contributions.

Paul Wormeli – Executive Director of the Integrated Justice Information Systems (IJIS) Institute

Peter Gnas – Network Manager with the Milwaukee Police Department

Pat Thetford – AT&T

Industry
Members:



Alcatel-Lucent



at&t



OnBase
a Hyland Software solution

Microsoft

QUEST
SOFTWARE