Justice Information Sharing Initiatives

A White Paper Prepared for the Attorney General's Advisory Committee of United States Attorneys by the Office of Justice Programs
October, 2004

Executive Summary

Winning the war on terrorism requires unprecedented levels of cooperation and unity of purpose across all levels of government. Following September 11, 2001 numerous initiatives were launched or expanded at the local, state, tribal and federal levels to improve our ability to "connect the dots." This paper describes some major ongoing justice information sharing initiatives that are being implemented at all levels of government and across the nation.

At the national policy level several key organizations and programs are poised to shape and guide the direction of justice information sharing:

- The **Global Justice Information Sharing Federal Advisory Committee (Global)**, is a consortium of 32 local, state, federal, and international organizations seeking to provide a "global" view on justice information sharing. Global reports to the Attorney General through the Assistant Attorney General, Office of Justice Programs.
- Global is implementing a **National Criminal Intelligence Sharing Plan (NCISP)** to develop national criminal intelligence sharing policies, procedures, standards, technologies, and training.
- The **Global Justice XML Data Model** provides a model and tools to help justice agencies across the country quickly and effectively develop applications that can share information across disparate computer systems and networks.
- The Department of Justice's **Law Enforcement Information Sharing Plan** is a Department-wide plan to facilitate law enforcement collaboration across agency and jurisdictional boundaries, in support of the National Criminal Intelligence Sharing Plan.
- **SAFECOM** is the federal government's coordinating organization for wireless voice communications interoperability among local, tribal, state, and federal public safety and first responder agencies.
- The **Law Enforcement Information Technology Standards (LEITS) Council** is a partnership between four of the nation's leading law enforcement associations and the Bureau of Justice Assistance, Office of Justice Programs, to involve law enforcement practitioners in the development of information technology standards for law enforcement.
- A proposed **National Intelligence Director (NID)** will serve as the President's primary intelligence advisor and also as head of the federal intelligence community.
- A central **National Counterterrorism Center (NCC)** was established by Executive Order to be a central repository for intelligence pertaining to terrorism and counterterrorism (excluding purely domestic counterterrorism).

- A new civil liberties advisory board was established by Executive Order and will counsel the President on effective means to ensure that the freedoms, civil liberties, and privacies that are legally protected by federal law are in fact protected in the performance of national and homeland security activities.

Some major technology systems in place include:

- The **National Law Enforcement Telecommunications System (NLETS)** supports data communications links to state networks using a commercial frame relay service.
- The **Homeland Security Information Network (HSIN)**, which is available in all 50 states, makes real-time threat-related information available to law enforcement and emergency managers on a daily basis through a Web-based system.
- The **Regional Information Sharing System (RISS)** links law enforcement agencies throughout the nation, providing secure communications, information sharing resources, and investigative support to combat multi-jurisdictional crime and terrorist threats.
- The FBI's **Law Enforcement Online (LEO)** is a national interactive computer communications system and information service, an Intranet exclusively for the law enforcement community. In 2003, it was linked to RISS, in order to improve the ability of each system to serve its constituency.
- The **Criminal Information Sharing Alliance Network (CISAnet)** provides information on distribution of illegal drugs, money laundering, weapons violations, sex offenders, missing persons, criminal histories and homeland security initiatives to participating state and local law enforcement organizations in the Southwest United States.
- **Open Source Information System (OSIS)** is an unclassified intranet run by the intelligence community.

This paper also summarizes some innovative regional information sharing projects like Minnesota's CriMNet, Chicago's CLEAR, and Washington DC's CAPWIN.

Funding is an issue for information sharing projects. Sources of potential funding within the Departments of Justice and Homeland Security are discussed, as are some ideas for creative approaches to funding information sharing projects.

As leaders in the justice community, U.S. Attorneys are well-positioned to enhance information sharing by working with the Anti-Terrorism Advisory Councils (ATAC) and the Law Enforcement Coordinating Committees (LECC) to put in place policies, structures and training to improve information sharing. U.S. Attorneys should also, where possible, take advantage of existing Department of Justice information sharing programs and technologies such as the National Criminal Intelligence Sharing Plan, the Global Justice XML Data Model, the Regional Information Sharing System, the FBI's Law Enforcement Online and the Homeland Security Information Network.

Introduction

In a February 2003 speech, President George W. Bush pledged to make information sharing at the local law enforcement level an important tool in the nation's war on terror. "All across the country we'll be able to tie our terrorist information to local information banks so that the front line of defeating terror becomes activated and real, and those are the local law enforcement officials. We expect them to be a part of our efforts; we must give them the tools necessary so they do their job."

Information sharing **will** have a huge impact in fighting crime and terrorism. However, for the uninitiated, the "alphabet soup" of acronyms describing various entities, initiatives and technology can be daunting. This paper is an attempt to clarify and summarize some key components of information sharing. To that end, it describes the various initiatives, the entities involved and their inter-relationships. It provides an introduction to key technology which can make information sharing and interoperability a reality, including the Global Justice XML Data Dictionary. It also describes a few sharing initiatives currently being implemented and it provides information on various funding sources for developing or improving information sharing within your region.

Global Justice Information Sharing Initiative (Global)

The Office of Justice Programs (OJP), a component of the United States Department of Justice, is deeply committed to encouraging information sharing at all levels, including state, local, regional, tribal, and Federal agencies. A primary instrument of the OJP involvement in information sharing is the **Global Justice Information Sharing Initiative**. This forms an umbrella that includes sharing of criminal intelligence information, as called for in the National Criminal Intelligence Sharing Plan (see below).

The Global Justice Information Sharing Initiative (Global) is a "group of groups," representing more than thirty independent organizations spanning the criminal justice spectrum at all levels of government, including law enforcement, the courts, corrections, probation and parole. This influential group works to address the many policy, privacy, connectivity, and jurisdictional issues that hamper effective justice information sharing. Global's mission is to promote the efficient, secure sharing of information among justice entities.

The Global Advisory Council (GAC) serves as an official advisory body to the U.S. Attorney General, and works through the Assistant Attorney General for the Office of Justice Programs to advise the Attorney General on justice information sharing issues. Through this counsel, Global promotes standards-based electronic information exchange to provide the justice community with timely, accurate, complete, and accessible information in a secure environment. The GAC includes representatives from 32 criminal justice organizations and operates under the auspices of, and is staffed by, the Office of Justice Programs (OJP), U.S. Department of Justice.

Global aids its member organizations and the people they serve through a series of important initiatives. These include the facilitation of the Global working groups, development of key technology standards, creation of white papers on data sharing issues, and the dissemination of information via the Global Web site. Global has produced a number of useful products, including the National Criminal Intelligence Sharing Plan and the Global Justice Extended Data Markup Language Data Model (both discussed below). Other products include the *Applying Security Practices to Justice Information Sharing* CD, a layman's guide to security in the information sharing environment.

In addition to members of the justice system, many other organizations from public safety, social services, and the private sector collaborate with Global through its working groups and affiliated programs. The primary work of Global is accomplished through four working groups: the Global Infrastructure/Standards Working Group, the Global Security Working Group, the Global Intelligence Working Group, and the Global Privacy and Information Quality Working Group. More information is available at www.it.ojp.gov.

National Criminal Intelligence Sharing Plan (NCISP)

The National Criminal Intelligence Sharing Plan (NCISP) is a guide to help agencies establish criminal intelligence sharing policies, procedures, standards, technologies, and training. The NCISP contains 28 recommendations that address criminal intelligence sharing needs. It sets forth standards for sharing data and handling security, policy and procedure blueprints for administrators, and technology architecture for readily sharing Sensitive but Unclassified (SBU) information.

The NCISP was first envisioned by a summit convened in March, 2002, by the International Association of Chiefs of Police (IACP). It was developed by the Global Intelligence Working Group, approved by the GAC, and submitted to the Attorney General in September 2003. It has been enthusiastically endorsed by Attorney General Ashcroft, and work is underway to implement the Plan.

Global Justice XML Data Model

Extensible Markup Language, or XML, provides a basic structure and set of rules for labeling the information in a document so that it can be read by any other computer. XML is an open standard for describing data. It defines data elements on Web pages and business-to-business or government-to-government documents. It is similar to HTML, but HTML defines how data elements are displayed, while XML defines the meaning and relationship of the data elements. Where HTML deals with format, XML deals with meaning. XML also allows the developer to define data or "tags" for any type of data exchange. As an example, if a word for an object did not exist within the English language, we would go though a process of adding a new word to our lexicon. XML allows for this kind of tag and language with a basic set of rules so that computers can more easily exchange data.

XML has been recognized as a worldwide standard for information processing, and industries that use information to drive their everyday operations have been early advocates of XML. In 2003, the Society of Worldwide Interbank Financial Telecommunications (SWIFT), a global cooperative of more than 7,000 financial institutions, agreed to develop a single XML standard for sending payment information. This single commitment is projected to affect how trillions of dollars change hands and to create enormous savings for the industry in information technology and business costs. The Department of Justice is seeking to generate similar benefits for agencies fighting crime and terrorism by encouraging the adoption of the Global Justice XML Data Model.

The Global Justice XML Data Model (GJXDM) provides reusable application components, honed to meet the needs of the justice community, that were built using international XML standards to facilitate information sharing across disparate computer systems and networks. GJXDM is an object-oriented data model that comprises approximately 2,500 data objects. Each object is made up of number of data elements or "tags." These objects facilitate the exchange and reuse of information from multiple sources and applications by defining and standardizing the information which can be shared by all of the justice and public safety communities. These data define everything from booking slips to court documents, such that, although they are created and stored in different formats, their information content can be easily shared with other systems and merged into a comprehensive information system. Furthermore, as new needs are identified, new data objects may be added to meet the needs of the justice and public safety community.

Today more than 50 justice information sharing projects across the nation are being implemented with the Global Justice XML Data Model including the DOJ LEISP, Minnesota's CriMNET, Pennsylvania's JNET™, and the FBI's N-DEx program. More information on the data model is available at www.it.ojp.gov.

Justice Information Exchange Model (JIEM)

Although not directly a Global project, the Justice Information Exchange Model (JIEM) Project is helping to simplify implementation of information sharing systems using the GJXDM. JIEM, run by SEARCH and funded by the Bureau of Justice Assistance, Office of Justice Programs, is designed to facilitate the design, planning, and implementation of integrated justice information systems by assisting in the development of models that illustrate how information is shared and distributed. The JIEM Modeling Tool© is a web-based software application that, when combined with a provided methodology, allows users to capture detailed information regarding the information flow and rules associated with integrated justice information systems and then provides developers with virtually all of the information they need to develop these systems. This can result in substantial savings for projects that use the tool, along with a greater confidence that all necessary information will be carried from one stage of the justice system to the next.

The latest version of the JIEM Modeling Tool© was developed with technical assistance from the Georgia Tech Research Institute (GTRI). GTRI is working with Global on the GJXDM, and the latest JIEM Modeling Tool is designed to interface to the GJXDM. This greatly simplifies bringing Justice XML data standards to participating sites. More information can be found at www.search.org/programs/technology/jiem.asp.

Other Key Programs and Their Relationships

In addition to Global, there are a number of other programs that address the issue of information sharing.

Criminal Intelligence Coordinating Council (CICC)

One of the primary recommendations of the NCISP was the creation of a Criminal Intelligence Coordinating Council (CICC) that would be representative of federal, state, local and tribal law enforcement and that would oversee the implementation of the NCISP, advising the federal government broadly on information sharing issues. The CICC will develop national-level policies to implement the NCISP and monitor the progress of the NCISP on the state and local level. The CICC will work with the Department's Law Enforcement Information Sharing Program and with the Justice Intelligence Coordinating Council (JICC) to improve the flow of intelligence information among federal, state, and local law enforcement agencies. It has also assumed a role in advising the Department of Homeland Security, as well as the Department of Justice, on the sharing of homeland security-related SBU information.

Executive Office for U.S. Attorneys and Global

The Executive Office for U.S. Attorneys (EOUSA) has been an active part of Global since 2000. EOUSA is one of the 30 member organizations of the Global Advisory Committee (GAC). The EOUSA is currently represented on the GAC by Ms. Jeanette Plante, Special Assistant United States Attorney, currently on detail to the EOUSA.

There are many organizations that are not members of the GAC but that actively participate in the efforts of the previously mentioned Working Groups. The EOUSA is currently also represented on one of these working groups by Ms. Plante, who serves as Vice-chair of the Global Privacy and Information Quality Working Group.

Law Enforcement Information Sharing Program (LEISP)

As part of its commitment to the National Criminal Intelligence Sharing Plan and to information sharing in general, the U.S. Department of Justice as a whole is committed to expanding the sharing of information, both among agencies within the Department and between the Department and state, local, and regional agencies. This commitment is being formalized through the Law Enforcement Information Sharing Program.

The Law Enforcement Information Sharing Program (LEISP) is a Department-wide plan to facilitate law enforcement collaboration across agency and jurisdictional boundaries. Its key components are enhancing access to law enforcement information for authorized users; improving information sharing within the Department and among the Department's federal, state, and local law enforcement partners; and coordinating departmental information sharing projects.

LEISP is DOJ's strategy to support law enforcement information sharing, and includes changes in the internal information infrastructure across the Department, including operational agencies such as the FBI and ATF. All agencies within the department will share information freely as part of normal policy. In addition, LEISP provides a framework for also sharing information readily with state, local, regional, and tribal agencies, initiatives and networks.

The LEISP strategy is still being developed. The strategy will not consolidate all information or responsibility at the federal level. It will not displace existing information sharing efforts at the local, regional, state or tribal levels. Instead, it is intended to facilitate the linking of existing systems to enhance further the sharing of information.

SAFECOM

SAFECOM's mission is to serve as the umbrella coordinating organization within the federal government for wireless voice communications interoperability focusing on local, tribal, state, and federal public safety and first responder agencies. Voice communications interoperability is the ability of public safety agencies to talk across disciplines and jurisdictions via radio communications systems, exchanging voice with one another on demand, in real time, and when authorized. As a public safety practitioner-driven program, SAFECOM, housed in the Department of Homeland Security's Science & Technology Directorate, is working with existing federal communications initiatives and key public safety stakeholders. Its purpose is to address the need to develop better technologies and processes for the cross-jurisdictional and cross-disciplinary coordination of existing systems and future networks. Complementing SAFECOM's efforts, the National Institute of Justice's CommTech program (formerly known as AGILE) is a research and development program bringing new technologies that address both voice and data interoperability to the first responder community.

Law Enforcement Information Technology Standards (LEITS)

The Law Enforcement Information Technology Standards (LEITS) Council is a partnership among four of the nation's leading law enforcement associations—the National Sheriffs' Association, Police Executive Research Forum, International Association of Chiefs of Police, and National Organization of Black Law Enforcement Executives—and the Bureau of Justice Assistance to involve law enforcement practitioners in the development of information technology standards for law enforcement. The LEITS Council works to foster the strategic development of integrated justice systems through the definition and implementation of standards. The LEITS Council is focusing on facilitating the development of functional standards for Computer Aided Dispatch (CAD) and Records Management Systems (RMS). The council has developed a strategy that will use committees composed of members of the law enforcement and vendor communities and other CAD and RMS experts to validate the functional requirements.

National Intelligence Director and Recent Executive Orders

National Intelligence Director

The proposed National Intelligence Director (Director), created by Executive Order of the President, will serve as the President's primary intelligence advisor and as head of the federal intelligence community. The Director will be given roles and responsibilities that will better enable the intelligence community to provide an integrated intelligence product. The Director will help ensure that the President has the best possible assessments from intelligence professionals.

Recent Executive Orders

On August 27, 2004, the White House released four Executive Orders related to terrorism. These Executive Orders are directed at federal agencies. The President cannot direct the actions of other agencies, including state, local, or tribal agencies. Nonetheless, there is potential for these

Orders to impact state, local, tribal, or regional information sharing efforts. Of particular interest in this context are the Executive Orders for:

- National Counterterrorism Center
- Establishing the President's Board on Safeguarding Americans' Civil Liberties
- Strengthening the Sharing of Terrorism Information to Protect Americans

National Counterterrorism Center

A central National Counterterrorism Center (NCC) was established by Executive Order. The NCC is charged with being a central repository for intelligence pertaining to terrorism and counterterrorism (excluding purely domestic counterterrorism). The NCC will also be the center for strategic planning of intelligence operations, including assigning primary responsibilities and ensuring that all executive agencies will have and provide appropriate access to all-source intelligence support. State and local agencies are mentioned, as part of the policy states that executive agencies "shall give the highest priority to … the interchange of terrorism information between [federal] agencies and appropriate authorities of States and local governments…." In addition, the Order provides for the NCC to receive, retain, and share information from all sources, including state and local governments.

Many other efforts (some mentioned elsewhere in this document) are already underway to coordinate sharing of information at all levels.

Establishing the President's Board on Safeguarding Americans' Civil Liberties Primary responsibilities and tasks

This Order establishes a new civil liberties board that will advise the President on effective means to ensure that freedoms, civil liberties, and privacies that are legally protected by federal law are in fact protected in the performance of national and homeland security activities.

Although there are no explicit references to state, local or tribal agencies, these may be impacted by policies that are established by the board, if these policies regulate the sharing of information among federal and state, local, regional, or tribal agencies. The Order does allow for the board, the Attorney General, or the Secretary of Homeland Security to establish committees that include "individuals from outside the executive branch of the federal government," thus opening the way for input from non-federal levels. The U.S. Attorneys may be well-positioned to provide valuable input based on their interactions with state and local agencies.

Strengthening the Sharing of Terrorism Information to Protect Americans

This Order requires that federal agencies will design and use information systems in a manner that maximizes sharing of information related to terrorist activities. Like the previously discussed Order, this one includes "the interchange of terrorism information between [federal] agencies and appropriate authorities of states and local governments …." The heads of all federal agencies which possess terrorism information are directed to share the information as appropriate.

Standards for sharing terrorism information are to be established. Many of these needs are addressed in the National Criminal Intelligence Sharing Plan. The standards further require that shared terrorism information be free of originator controls (e.g., requiring the consent of the originating agency to further share information). Many state or local jurisdictions have their own legal requirements that bind information sharing, and these will need to be respected and addressed.

This Order has the potential for substantial impact in the state and local arena, as well as the federal arena. The Order directs the federal agencies to minimize the classification and compartmentalization of data, which may result in a much greater flow of information from federal agencies to state, local, regional, and tribal systems.

Justice Information Sharing Networks

Information sharing is accomplished by using networks and systems that are able to provide appropriate security and functionality for the exchange of law enforcement and justice information. These networks may vary in the functionality provided, depending in part on their target audience. Representatives of many of these systems participate in the various activities of Global. What follows is a very brief description of some of the more prominent networks currently in place.

National Law Enforcement Telecommunications System (NLETS)

The National Law Enforcement Telecommunications System (NLETS) began operation in 1966 as the Law Enforcement Teletype System. Today, NLETS provides two basic capabilities:

- A computer-based message switching system linking together state, local and federal law enforcement and justice agencies for the purpose of information exchange
- Information services support for justice-related applications

NLETS supports data communications links to state networks using a commercial frame relay service, not the Internet. Within each state, all agencies receive NLETS service through the state interface. Federal and international systems gain access in a similar manner. Users of NLETS include all of the states and territories, all federal agencies with a justice component, and even some international agencies. Data that are shared through NLETS transactions (requests for information and returned data) range from motor vehicle and driver records, to HAZMAT and GSA Federal registrations, to Canadian "Hot File" records and INS databases to state criminal history records. Over 40 million messages are transacted each month.

Homeland Security Information Network (HSIN)

The Homeland Security Information Network (HSIN), which is available in all 50 states, makes real-time threat-related information available to law enforcement and emergency managers on a daily basis through a Web-based system. Members of the private sector, including owners and operators of critical infrastructure, now also receive threat-related information through the HSIN system. In addition, members of 35 different Federal agencies are now all co-located in DHS' new 24-hour Homeland Security Operations Center, which allows the information coming from various sources to be synthesized together and then shared with other federal partners such as the FBI and the Department of Defense. In addition, nearly 100 bulletins and other threat related communiqués have been sent to homeland security professionals across the country.

The system is encrypted at the most secure levels, ensuring the safest delivery of real-time interactive connectivity among state and local partners through the Department's Homeland Security Operations Center (HSOC) using the Joint Regional Information Exchange System (JRIES), a secure network and a suite of applications including mapping and imaging capabilities. It is centered on addressing four basic needs, including planning and preparedness, emergency response, threat awareness and vulnerability identification, and basic information sharing. Major features include broadcasting and "narrowcasting" of warnings and threats from DHS, user access to sensitive documents that enables real-time analysis of data, secure e-mail, and provision of peer-to-peer collaboration technology allowing real-time dialogue among members.

Each state and major urban area's participants includes governors, mayors, Homeland Security Advisor, state National Guard offices, Emergency Operations Centers, First Responder and Public Safety departments, and other key homeland security partners. Each receives software licenses, technology, and training to participate in combating terrorism, enhance information sharing to combat terrorism and increase anti-terrorism situational awareness.

Joint Regional Information Exchange System (JRIES)

Originating as a pilot project by the Department of Defense (DOD)'s Defense Intelligence Agency (DIA) aimed at improving the exchange of counterterrorism information between local and state law enforcement and components of DOD and DIA, the Joint Regional Information Exchange System (JRIES) is an Internet-based counterterrorism communications initiative. Now managed as an application on the Department of Homeland Security's (DHS) Homeland Security Information Network (HSIN), the JRIES target audience includes state and local governments, counterterrorism and intelligence agencies, and law enforcement agencies. Operating at the sensitive but unclassified (SBU) level, JRIES facilitates collaboration among its members by providing a secure environment for exchanging emails and peer-to-peer collaboration allowing real-time dialogue, and also provides access to data visualization software and analysis tools. It has also provided real-time links between the Homeland Security Operations Center and counterterrorism teams at high-profile events such as this year's Super Bowl and Sugar Bowl football games.

Regional Information Sharing System (RISS)

The Regional Information Sharing System (RISS), which was created by Congress in 1974, links law enforcement agencies throughout the nation, providing secure communications, information sharing resources, and investigative support to combat multi-jurisdictional crime and terrorist threats. RISS is a national program made up of six centers that operate in geographic regions of varying size, serving the unique needs of law enforcement in each region while fostering information sharing among all levels of law enforcement across the country. RISS serves over 7,000 local, state, federal, and tribal law enforcement member agencies in all 50 states, the District of Columbia, U.S. territories, Australia, Canada, and England. Formed primarily by state and local law enforcement officials, RISS is governed by a board representative of its membership. It is an entity independent of the federal government, but serving all levels of government. Since its inception, RISS has been supported by funding from DOJ/OJP, in addition to membership dues.

The RISS secure intranet — RISSNET— serves as the communications backbone for the secure exchange of sensitive information and also allows instant electronic access to RISS services by RISS member agencies. Resources available for access on RISSNET include the RISS Investigative Leads Bulletin Board; RISSLive; the RISS criminal intelligence databases (RISSIntel); various state, regional, federal, and specialized criminal intelligence databases; the RISS National Gang Database; the RISS Anti-Terrorism Information Exchange (ATIX); RISS center Web sites; the RISS search engine (RISSSearch); and the newest resource available on RISSNET called RISSLinks–a data visualization and link analysis tool. Member agencies may also contact center staff directly to request assistance in database records searches, use of other RISS services such as analytical assistance on cases, obtaining loan of specialized surveillance equipment, confidential funds support, obtaining criminal activity bulletins and publications, and obtaining contact information on officers in other agencies that may assist in furthering an investigation.

Law Enforcement Online (LEO)

The FBI's Law Enforcement Online (LEO) is a national interactive computer communications system and information service, an Intranet exclusively for the law enforcement community. It is a user-friendly service which can be accessed by any approved employee of a duly constituted local, state, or federal law enforcement agency, or approved member of an authorized law enforcement special interest group. LEO is intended to provide a state-of-the-art communication mechanism to link all levels of law enforcement throughout the United States. LEO is also used as a vehicle to educate officers on the best technologies and practices in all areas of law enforcement. Online services available to members include special interest group bulletin-boards, customized web-pages focused on law enforcement subjects, chat, email, electronic calendar, topical electronic library and distance learning services.

RISS-LEO collaboration

On September 1, 2002, the FBI's Law Enforcement Online (LEO) and the RISSNET established an electronic interface that enables registered users to access both systems with a single log-on. A major benefit of the RISSNET/LEO partnership is that privileges that have been granted on one system are automatically extended in an appropriate manner to users of the other system. In addition to secure e-mail and communications, LEO provides access to still more databases of great interest to various groups in law enforcement, particularly the Bomb Data Center, the Hostage/Barricade System, and the Law Enforcement and Intelligence Agency Linguist Access.

RISS/ATIX

(http://www.rissinfo.com/rissatix.htm)

In April, 2003, RISS expanded its services and implemented the Anti-Terrorism Information Exchange (ATIX) to provide users outside the law enforcement community, including public health organizations, fire departments and other non-law enforcement first responders, and even public utilities and school systems with access to homeland security, disaster, and terrorist threat information. RISS member agencies as well as executives and officials from other first responder agencies and critical infrastructure entities can access ATIX, which will provide access to RISSNET secure Web pages, databases, collaborative capabilities, secure e-mail and bulletin boards.

Much of the information on RISSNET is law enforcement sensitive, so ATIX includes safeguards to ensure that users are only able to access information appropriate to their particular user role and community. Because it is part of RISSNET, ATIX also will be linked to the Open Source Information System network under development at the federal level, giving the larger homeland security community at the state and local levels access to even more resources.

Criminal Information Sharing Alliance Network (CISAnet)

The Criminal Information Sharing Alliance Network (CISAnet) was formerly known as the Southwest Border States Anti-Drug Information System (SWBSADIS). CISAnet originally began as part of the U.S. effort to suppress the distribution of illegal drugs. It has expanded to include information sharing on money laundering, weapons violations, sex offenders, missing persons, criminal histories, and a number of homeland security initiatives. This system is based on trust relationships and acts as an honest broker to provide users real-time bidirectional query access across all of the connected systems.

CISAnet is a "network of networks" connecting state and local law enforcement organizations in the participant states (Arizona, California, Georgia, Idaho, New Mexico, and Texas). Connectivity of the otherwise disparate systems is possible because of a focus on the use of standard interface, allowing participant infrastructure investments to be reused.

Open Source Information System (OSIS)

The Open Source Information System (OSIS) is an unclassified intranet run by the intelligence community. OSIS provides for the exchange of unclassified U.S. Government information, commercial databases containing the text of articles from a wide range of periodicals and publications, and translations of a wide range of media reports in more than 70 languages. In addition to this "open source" information, OSIS provides an environment for access to some Sensitive but Unclassified (SBU) information that may be of interest to the intelligence community. OSIS offers tools to assist users in analysis and graphical interpretations of data. OSIS can also provide near-real time translations of foreign language web pages. Worldwide dial-in access is provided, along with secure, encrypted email for users within the OSIS. Secure Virtual Private Network (VPN) technology is used to provide a protected environment for intelligence community users to share unclassified data and tools, communicate with one another, and access the internet in a secure manner.

Relationships between the Networks

Some may view these networks as competing entities. In fact they should be viewed in many cases as being complementary. For example, while RISS and LEO are both primarily law enforcement-oriented systems, the RISS -LEO system addresses a much wider spectrum of criminal activity than does the counterterrorism-focused HSIN. However, even within the counterterrorism mission, HSIN and RISS-LEO are complementary programs. In addition, they share an interface that allows users to have ready access to both systems. For example, the HSIN will post its daily reports and warnings directly to RISSNET/LEO through the JRIES interface.

RISS-LEO and OSIS are connected as well. This allows more civilian law enforcement agencies access to OSIS, where the intelligence community centralizes all of the unclassified homeland security information it has gathered. RISS-LEO and CISAnet have forged links between their systems. Finally, RISS-LEO and the NLETS systems are testing a transparent interface between their respective systems.

RISS-LEO is the subject of one of the NCISP recommendations. Specifically, it is recommended that RISS-LEO "provide the initial sensitive but unclassified secure communications backbone for implementation of a nationwide criminal intelligence sharing capability." However, additional systems have been developed in the interim, such as the HSIN, so the Departments of Justice and Homeland Security are working together to create such a communications backbone capable of linking all of these systems.

A sampling of other information sharing initiatives

There are many active information sharing initiatives throughout the United States. The approaches used are varied. Many of these arose as the result of a determination by people in a discrete geographic area that they needed to share information in order to meet various needs of their communities in a more effective manner. As a result, the size and scope of the sharing varies, both in terms of geography and in the types of information and services shared. In some cases, smaller initiatives or programs may even become part of a larger system that is sharing information.

What follows is a brief discussion of just a few of the many ongoing projects. This list does not constitute an endorsement of any of these systems, nor should an omission of an initiative suggest that that initiative is not meeting needs.

Minnesota Integrated Criminal Justice Information System (CriMNet)

Minnesota CriMNet is an enterprise architecture that puts in place a statewide framework of people, processes, data, standards, and technology focused on providing accurate and comprehensive data to the criminal justice community in the State of Minnesota. The CriMNet integration effort is not one single project, but incorporates many projects that are being developed by criminal justice organizations throughout Minnesota. The integration architecture is driven by local operational needs and uses standards that will support the exchange of data across existing and developing systems.

Once completed, CriMNet will link the more than 1,100 jurisdictions within Minnesota. CriMNet is a secure system that will allow authorized users to retrieve and search selectively entered information from every jurisdiction of the state, including criminal history data, probation status, and arrest photos. As this system moves forward, hiding places for criminals will be eliminated, crimes will be solved, and communities will become safer. Six major Minnesota networks have already been implemented on CriMNet: Court Web Access, Statewide Supervision System, Minnesota County Attorney Practice System, Predatory Offender Registry, Minnesota Repository of Arrest Photos, and Prison Adapter.

Law Enforcement Information Exchange (LInX)

In the Puget Sound region, the Law Enforcement Information Exchange (LInX) system is being financed by the Naval Criminal Investigative Service (NCIS). The data warehouse-based LInX will allow law enforcement agents to access information from a range of databases belonging to law enforcement agencies in Seattle, Kitsap, Snohomish and King counties in Washington, the

Washington State Patrol and Washington Jail Booking and Records System, and the NCIS. LInX will warehouse a wide variety of information, ranging from street officers' field interview reports and observations to arrest records. In addition to simple searches, it can analyze these records and provide some link analysis in seconds, allowing law enforcement quickly to recognize patterns of suspicious behavior. Users will be able to access information in the data warehouse securely using a standard Web browser.

Automated Regional Justice Information System (ARJIS)

The Automated Regional Justice Information System (ARJIS) is an integrated criminal justice network used by 50 local, state and federal agencies in the San Diego region. ARJIS supports a regional enterprise network capable of linking to all criminal justice systems in the region. The ARJISNet secure intranet provides secure access to a wide variety of regional criminal justice data. In addition to connecting more than 10,000 users, ARJIS is used for tactical analysis, investigations, statistical information, and crime analysis, and allows law enforcement agents to receive electronic notification if another agency or officer obtains information related to an individual, location or vehicle. The key to success has been that ARJIS provides "single point of entry" access to query all regional justice data, regardless of the system in which it is stored. ARJIS is taking advantage of this ability in pilot efforts to provide wireless field access to critical law enforcement data via hand-held PDAs.

Citizen and Law Enforcement Analysis and Reporting (CLEAR)

Another large initiative is Chicago's Citizen and Law Enforcement Analysis and Reporting (CLEAR) system. In the three years since Chicago police began operating CLEAR, the city has experienced a 16% decline in murders, rapes, robberies and other crime. CLEAR includes the 132 police jurisdictions in Cook County, Illinois (including federal law enforcement agencies). It provides an integrated criminal justice records system, thus simplifying some aspects of information sharing. The CLEAR system provides real-time information of value to 25,000 law enforcement officials at all levels. Users can draw upon a system that holds information and digital photos on 7 million offenders and 3 million incidents. In addition to providing "classic" information such as warnings related to incident reports and warrants, CLEAR can also conduct link and pattern analysis. The Chicago Police Department and the Illinois State Police are also piloting wireless access to CLEAR statewide.

Though implementation of the communications network for CLEAR is still incomplete, the Chicago and Illinois State Police agencies have begun the process of consolidating the CLEAR system with Illinois' statewide Law Enforcement Agencies Data System (LEADS) to create one integrated technology solution to serve all law enforcement in the state. This new project known as I-CLEAR is scheduled to come online in December 2004. I-Clear will provide law enforcement throughout the state with a predictive analytical tool that has access to CLEAR data ; LEADS 36-year database of missing persons, gang members and criminal records; the FBI's National Crime Information Center; and NLETS.

Multistate Anti-Terrorism Information Exchange (MATRIX)

The Multistate Anti-Terrorism Information Exchange (MATRIX) Program is a pilot data warehouse-based effort that will initially connect state criminal indices and investigative file databases, driver's license and motor vehicle registration databases, and numerous other public data records, allowing for rapid combined data query and sharing among law enforcement participants. No new data are being made available to law enforcement, but the speed of the access is greatly improved. Database applications and information sharing performed through MATRIX are carefully structured to be in compliance with the laws of each participating state, and are to be used only as part of criminal investigations. The system is connected using an existing network, the Sensitive but Unclassified (SBU) RISSNET secure intranet. Current participating states include Michigan, Ohio, Pennsylvania, Connecticut, and Florida.

Gateway Information Sharing Initiative

Another data warehouse-based initiative is the Federal Bureau of Investigation's (FBI) Gateway Information Sharing Initiative (Gateway Project) pilot project in the St. Louis, Missouri area. It has also been piloted in other locations, including San Diego, California. Investigative files and records from all levels of law enforcement are merged into a single data warehouse, and data are then available to all participating agencies for sophisticated search and analysis. The Gateway ISI marks the first time the FBI has entered records in a data warehouse that contains investigative data from local and state law enforcement agencies. The Gateway Project was a prototype for a national system called the Multiple Agency Information Sharing Initiative, which will provide a national database of case files. The Gateway Project also includes a classified data warehouse that adds classified FBI counterterrorism investigative data to the sensitive but unclassified holdings for exploitation by interagency members of the Joint Terrorism Task Force in the FBI field division.

CapWIN – Information sharing beyond the public safety community

The Capital Wireless Integrated Network (CapWIN) began in 1999 as a partnership between the states of Maryland and Virginia and the District of Columbia. The project was developed to respond to the inability of neighboring jurisdictions in the Washington, D.C. metropolitan region to communicate at incident scenes. The purpose of CapWIN is to develop an integrated criminal justice and transportation information wireless network. Once implemented, this project will integrate transportation and public safety communication systems (data and voice) in the two states and Washington, D.C. The primary goal of this project is to have multiple mobile data platforms communicating seamlessly across the network, regardless of jurisdiction or geographical location. CapWIN's targeted users include federal, state, and local police; fire; and EMS vehicles, as well as state Department of Transportation service patrols. The system will provide critical information to transportation and public safety agencies during major incidents as well as during daily operations in this area.

Project Seahawk

Project SeaHawk was created as a benchmark project to enhance the protection, security, and infrastructure of seaports nationally. Administered by the U.S. Attorney's Office for the District of South Carolina, Project SeaHawk is focused on the Port of Charleston, South Carolina, the second largest container port on the east coast and fourth largest in the nation. Project SeaHawk comprises 47 agencies involved with port -related activities, including law enforcement agencies at a variety of levels. SeaHawk has linked databases and physical security systems in a comprehensive system. In its next phase, Project SeaHawk will add new technologies that will result in a system that truly integrates all information and physical security systems into one coherent fused system. In addition, Project SeaHawk will address more specialized issues related to maritime transportation systems and centers.

Pennsylvania' Justice Network (JNET™)

Pennsylvania's Justice Network (JNET™) is a secure virtual system for the sharing of justice information by authorized users. JNET™ is a collaborative effort of municipal, county, state, bordering states and federal justice agencies to build a secure integrated justice system. JNET™ provides a common on-line environment whereby authorized users can access offender records and other justice information from participating agencies. Based on open Internet/World Wide Web technologies and standards, JNET™ links information from diverse hardware and software platforms under a common, web-browser interface. Firewalls protect agency networks and systems from unauthorized intrusion. JNET™ has avoided "turf issues", which have traditionally plagued other integration efforts, by leveraging existing agency systems, recognizing and ensuring agency independence, and allowing agencies to maintain control of their information. As of August 2004, JNET™ connected 53 counties and 12 agencies with 6,748 county users and 4,211 federal and state users.

Law Enforcement National Data Exchange (N-DEx)

The Law Enforcement National Data Exchange (N-DEx) System, under development by the FBI's Criminal Justice Information Services Division (CJIS), will be an incident/event based nationwide information sharing system for local, state, tribal, and federal law enforcement agencies. It will securely collect and process criminal data in support of investigations, crime analysis, law enforcement administration, strategic/tactical operations and national security responsibilities. N-DEx will provide law enforcement with access to information such as methods of criminal operation identified by national contributors, arrestee/indicator information, victim information, suspect information, and other ongoing criminal and investigative information, as well as pointers to more detailed indices and case information. In addition, N-DEx will provide an automated tool to help identify linkages between various incidents. These links can then be used to query the National Crime Information Center (NCIC), the Interstate Identification Index (III), and other criminal justice information that may be contained in N-DEx, to determine if relationships exist and return this information to participating agencies.

National Virtual Pointer System

The Drug Enforcement Administration (DEA), in partnership with the High Intensity Drug Trafficking Area Program and the Regional Information Sharing Systems (RISS), is developing the National Virtual Pointer System (NVPS). Using NVPS, participating agencies will be able to determine if any other law enforcement entity is focused on the same investigative target, regardless of the crime. A single entry will allow a user to access all participating pointer deconfliction databases. The user will then be linked to the agent or law enforcement officer who has information on the related case. NVPS will provide connectivity using the NLETS and RISSnet systems.

Regional Information Sharing Funding Opportunities

Sources within both the Department of Justice and the Department of Homeland Security distribute funding that can be used for criminal justice information sharing projects. The bulk of these funds are distributed to the states in block, or formula, grants (based on a formula taking into account population and other factors). For Office of Justice Programs (OJP) funding, you may visit the National Institute of Justice (NIJ) web site at www.ojp.usdoj.gov/nij/funding.htm, and the Bureau of Justice Assistance (BJA) web site at www.ojp.usdoj.gov/BJA/grant. Within the Department of Justice, you may also want to visit the Office of Community Oriented Policing web site, at http://www.cops.usdoj.gov. The Office for Domestic Preparedness, within the Department of Homeland Security, provides significant funding to the states and to major urban areas, usable for such items as information systems and communications interoperability; that agency's web site is http://www.ojp.usdoj.gov/odp.

Within OJP, BJA supports information sharing primarily through the Byrne Formula Grants and the Local Law Enforcement Block Grants (LLEBG). Byrne Formula Grant Program funds are awarded directly to state governments, which then set priorities and allocate funds within each state. The permissible uses of Byrne Formula Grant funding are quite broad, and would support, among other things, information sharing initiatives. In recent years, $500 million per year has been distributed to the states in Byrne Formula Grants. Of course, the amount available each year is subject to Congressional appropriation.

Significantly, for those wishing to enhance information sharing, it is useful to know that recipients of Byrne Formula Grant funding are required by statute to set aside five percent (5%) of their grant funds to improve criminal justice records in their states. These funds must be spent on programs that promote:

- The completion of criminal histories to include the final disposition of all arrests for felony offenses.
- The full automation of all criminal justice histories and fingerprint records.
- The frequency and quality of criminal history reports to the FBI.
- The improvement of state record systems.
- The sharing of all records described above with the U.S. Attorney General.
- The sharing of the child abuse crime records required under the National Child Protection Act of 1993 (42 U.S.C. 5119 et seq.).

BJA also awards funds to states and units of local government through the Local Law Enforcement Block Grant (LLEBG) Program. LLEBG Funds from the LLEBG program may be used for procuring equipment, technology, and other material directly related to basic law enforcement functions. More information about both Byrne Formula Grants Program and the LLEBG can be found at www.ojp.usdoj.gov/BJA/grant/byrne.html and www.ojp.usdoj.gov /BJA/grant/llebg_app.html.

Additionally, other OJP bureaus and program offices offer funding opportunities to enhance and improve criminal justice systems and services for crime victims. Visit the OJP grants and funding page at www.ojp.usdoj.gov/fundopps.htm.

The Office of Community Oriented Policing Services (COPS) offers funding to advance community policing services, including initiatives associated with regional information sharing projects. The COPS office has funded approximately nine million dollars for Chicago's CLEAR information sharing program. Information about funding opportunities through COPS can be found by visiting www.cops.usdoj.gov.

The Bureau of Justice Statistics (BJS) also provides direct funding and technical assistance to states through the National Criminal History Improvement Program (NCHIP). NCHIP was created to ensure that accurate records are available for use in law enforcement, including sex offender registry requirements, and to protect public safety and national security. This assistance is designed to promote participation in and improvement of the interface between states and the national records systems including:

- the FBI administered National Instant Criminal Background Check System (NICS)
- National Protection Order File
- National Sex Offender Registry (NSOR)
- the Integrated Automated Fingerprint Identification System (IAFIS)

The Department of Homeland Security's Office of Domestic Preparedness (ODP) has several technology grant programs including the Information Technology and Evaluation Program (ITEP) and the Urban Areas Security Initiative (UASI). ITEP is specifically interested in working through state and local public safety agencies to fund novel uses of existing, "state-of-the-market" information technology that will remove barriers and improve information sharing and integration. ODP awarded $9 million in September 2004 through the ITEP program to seven states and local justice information sharing projects for Alabama, Arizona, California, Washington DC, Hawaii, Maryland and Michigan. UASI has a broader mandate to provide financial assistance to address the unique planning, equipment, training, and exercise needs of large urban areas for dealing with terrorist acts. However, it does address the need for funding for hardware, software and internet-based systems that allow for information exchange and dissemination. Additional information concerning both ITEP and UASI can be found at www.ojp.usdoj.gov/odp/ grants_programs.htm.

The Department of Homeland Security has provided 15 million to the state of Ohio for the Ohio Local Law Enforcement Information-Sharing Network (OLLEISN) which is being implemented using the Global Justice XML Data Model. OLLEISN will serve as a standards-based information and communication network that will allow the 900+ Ohio local law enforcement agencies to electronically share information stored in local Record Management Systems (RMS) and CAD (Computer Aided Dispatch) systems in a centralized data repository.

Finally, among the permitted uses of the substantial block grant funding provided by DHS/ODP is information systems. Each state is required to develop a strategic plan for the expenditure of these funds. Every state should consider whether its needs include funding for an information system that will not only aid its homeland security efforts, but also its broader law enforcement efforts, which are often inextricable.

U.S. Attorneys Can Help!

As leaders in the justice community, U.S. Attorneys are well-positioned to enhance information sharing. A November, 2001, memo from Attorney General John Ashcroft to all U.S. Attorneys directed them to take prompt action to increase cooperation with state and local officials in the fight against terror. Each U.S. Attorney should utilize the Anti-Terrorism Advisory Council (ATAC) in his or her jurisdiction, and should work closely with the local Law Enforcement Coordinating Council (LECC) to put in place the structures, policies and training needed to enable effective communication among local, state, and federal law enforcement. In fulfilling the Attorney General's directive, U.S. Attorneys should, where possible, take full advantage of the technologies and programs already available and currently in use by the Department to facilitate information sharing such as RISS, HSIN, LEO and programs such as the National Criminal Intelligence Sharing Plan and Global Justice XML Data Model. They should also assist their state and local partners in identifying funding opportunities to further local, state and federal information sharing initiatives in their Districts and/or regions. State and local law enforcement should be made aware not only of the multiple sources of funding available to them, but also how they may be able to leverage such funding, even involving multiple communities, federal Districts, and states in a collaborative funding process using, for example, pooled block grant funding from multiple jurisdictions. U.S. Attorneys are needed to help develop and lead the appropriate partnerships and collaborative relationships required to ensure the success of national policy initiatives such as the National Criminal Intelligence Sharing Plan.

Glossary of Acronyms

Note that links and page numbers to sections of this document are provided for those topics that are discussed in greater detail in this document. Please note that not all of these are discussed in detail.

ARJIS	Automated Regional Justice Information System (pg 14)
ARJISnet	ARJIS secure intranet (pg 14)
ATAC	Anti-Terrorism Advisory Council
ATIX	RISS Anti-Terrorism Information Exchange (pg 11)
BJA	Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice
BJS	Bureau of Justice Statistics, Office of Justice Programs, U.S. Department of Justice
CAD	Computer Aided Dispatch
CapWIN	Capital Wireless Integrated Network (pg 15)
CICC	Criminal Intelligence Coordinating Council (pg 5)
CISAnet	Criminal Information Sharing Alliance Network (pg 12)
CJIS	FBI's Criminal Justice Information Services Division
CLEAR	Citizen and Law Enforcement Analysis and Reporting system (pg 14)
COPS	Office of Community Oriented Policing Services, U.S. Department of Justice
CriMNet	Minnesota Integrated Criminal Justice Information System (pg 13)
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security

DIA	Defense Intelligence Agency
DoD	Department of Defense
DOJ	Department of Justice
EOUSA	Executive Office for U.S. Attorneys
FBI	Federal Bureau of Investigation
GAC	Global Advisory Council (pg 3)
GJXDM	Global Justice XML Data Model (pg 4)
Global	Global Justice Information Sharing Federal Advisory Committee, or may refer to the committee and its efforts through the Global Justice Information Sharing Initiative (pg 3)
GTRI	Georgia Tech Research Institute
HIDTA	High Intensity Drug Trafficking Area
HSIN	Homeland Security Information Network (pg 9)
HSOC	Homeland Security Operations Center (pg 9)
HTML	HyperText Markup Language - the "language" used for web pages
IACP	International Association of Chiefs of Police
IAFIS	Integrated Automated Fingerprint Identification System
ITEP	ODP's Information Technology and Evaluation Program (pg 17)
JICC	Justice Intelligence Coordinating Council (senior level coordination mechanism for all intelligence related activities conducted by the U.S. Department of Justice and its subordinate organizations)
JIEM	Justice Information Exchange Model (pg 5)

JNET	Pennsylvania's Justice Network (pg 16)
JRIES	Joint Regional Information Exchange System (pg 10)
LECC	Law Enforcement Coordinating Council
LEISP	Law Enforcement Information Sharing Program (pg 6)
LEITS	Law Enforcement Information Technology Standards Council (pg 7)
LEO	Law Enforcement Online (pg 11)
LInX	Law Enforcement Information Exchange (pg 13)
MATRIX	Multistate Anti-Terrorism Information Exchange (pg 14)
NCC	National Counterterrorism Center (pg 8)
NCHIP	National Criminal History Improvement Program
NCIC	FBI’s National Crime Information Center
NCIS	Naval Criminal Investigative Service
NCISP	National Criminal Intelligence Sharing Plan (pg 4)
N-Dex	Law Enforcement National Data Exchange System (pg 16)
NICS	FBI's National Instant Criminal Background Check System
NID	National Intelligence Director (pg 7)
NIJ	National Institute of Justice, Office of Justice Programs, U.S. Department of Justice
NLETS	National Law Enforcement Telecommunications System (pg 9)
NVPS	National Virtual Pointer System (pg 16)

ODP	Office of Domestic Preparedness, U.S. Department of Homeland Security
OJP	Office of Justice Programs, U.S. Department of Justice
OLLEISN	Ohio Local Law Enforcement Information-Sharing Network
OSIS	Open Source Information System (pg 12)
RISS	Regional Information Sharing System (pg 10)
RISSNET	RISS secure intranet (pg 10)
RMS	Records Management Systems
SBU	Sensitive But Unclassified (Definition is not uniform but usually refers to information that warrants a degree of protection and control while also satisfying criteria for exemption from mandatory public disclosure)
SWBSADIS	Southwest Border States Anti-Drug Information System (pg 12)
UASI	ODP's Urban Areas Security Initiative (pg 17)
VPN	Virtual Private Network
XML	Extensible Markup Language