Preface

This interim report presents the Global Justice Information Sharing Initiative (Global) Intelligence Working Group (GIWG) preliminary recommendations for achieving the goals and objectives outlined in the International Association of Chiefs of Police (IACP) *Criminal Intelligence Sharing Report*. These recommendations are also in response to direction from the Bureau of Justice Assistance (BJA), the Global Advisory Committee (GAC), and the IACP for development of a National Criminal Intelligence Sharing Plan.

All recommendations contained within this report are preliminary and are presented in draft form. They represent the work products of the six committees that were formed out of the GIWG. The GIWG recommendations will primarily impact the law enforcement community, and to some degree, public safety entities that are provided access to the information.

Subsequent to the issuance of this interim report, the GIWG will continue to refine the recommendations and gather additional data as needed for the final report. GIWG meetings are scheduled for June 16-17, 2003, and September 9-10, 2003, in order to identify and resolve any outstanding issues prior to the completion of the final report to the Bureau of Justice Assistance (BJA) in October 2003.

Background

In fall 2001, law enforcement officials attending the annual IACP conference in Toronto, Canada, identified the need for a comprehensive assessment to identify the inadequacies of the intelligence process that, in part, led to the failure to prevent the tragic events of September 11. As a result, law enforcement executives and intelligence experts met together at the IACP Criminal Intelligence Sharing Summit held in Alexandria, Virginia, in March 2002, and articulated a proposal for an intelligence sharing plan that was in alignment with the President's initiative to develop a Cabinet-level agency to coordinate homeland security. The Summit participants envisioned local, state, and tribal law enforcement agencies fully participating with federal agencies to coordinate, collect, analyze, and appropriately disseminate criminal intelligence information across the United States to make our nation safer. Results of the Summit are documented in the August 2002 report entitled *Recommendations from the IACP Intelligence Summit, Criminal Intelligence Sharing: A National Plan for Intelligence-led Policing at the Local, State and Federal Levels.*[1]

The IACP *Criminal Intelligence Sharing Report* contained a proposal to create a National Criminal Intelligence Sharing Plan ("Plan"). The most central and enduring element of the Plan advocated by Summit participants was the recommendation for the creation of a Criminal Intelligence Coordinating Council comprised of local, state, tribal, and federal law enforcement executives.[2] The Council's mandate would be to establish, promote, and ensure effective intelligence sharing and to address and solve, in an ongoing fashion, the problems that inhibit it. In fall 2002, in response to this proposal, the U.S. Department of Justice, Office of Justice Programs (OJP), BJA, authorized the formation of the GIWG, one of several issue-focused working groups of the GAC[3]. Melvin J. Carraway, Superintendent of the Indiana State Police, was designated as Chair of the GIWG.

The initial meeting of the GIWG occurred in December 2002, in Atlanta, Georgia. The members and organizations represented at the meeting were selected by BJA, in consultation with the Global Executive Steering Committee, based on their backgrounds and broad experiences with criminal justice and criminal intelligence issues. These officials represent all levels of law enforcement, including practitioners, policymakers, and subject-matter experts. A membership list is contained in the appendix to this report *(Appendix A)*. In addition to local, state, tribal, regional, and federal law enforcement personnel, the individuals on the GIWG represent the following organizations and groups: IACP; International Association of Law Enforcement Intelligence Analysts (IALEIA); Justice Management Institute; Law Enforcement

[1] This document is available at: http://www.theiacp.org/documents/pdfs/Publications/intelsharingreport.pdf.

[2] IACP *Criminal Intelligence Sharing Report*, p. 6.

[3] The Global Justice Information Sharing Initiative, operating under the program management of the Bureau of Justice Assistance, serves as an advisory body to the federal government—specifically through the Attorney General of the United States and the Assistant Attorney General, Office of Justice Programs—to facilitate standards-based electronic information exchange throughout the justice and public safety communities. The Global Advisory Committee (GAC or "Committee") is comprised of key personnel from local, state, tribal, federal, and international justice and public safety entities, and includes agency executives and policymakers, automation planners and managers, information practitioners, and end users. GAC membership reflects the involvement of the entire justice community in information sharing. Global working groups, made up of Committee members and other subject-matter experts, expand the GAC's knowledge and experience. These groups are formed to address timely issues impacting justice information sharing; the GIWG is one of four working groups. For more information on Global, please visit http://www.it.ojp.gov/global/.

Intelligence Unit (LEIU); Major Cities Chiefs Association; National Conference of State Legislatures; National White Collar Crime Center (NW3C); National Sheriffs' Association (NSA); Prosecutors; and State Law Enforcement Intelligence Networks.

Chairman Carraway established the following Committees to address the goals and objectives outlined in the IACP *Criminal Intelligence Sharing Report*:

- **Policy Committee**, chaired by Thomas Frazier, Executive Director of the Major Cities Chiefs Association.

- **Privacy Committee**, chaired by Russ Porter, Special Agent in Charge, Iowa Department of Public Safety.

- **Standards Committee**, chaired by Peter Modafferi, Chief of Detectives, Rockland County, New York, District Attorney's Office.

- **Connectivity/Systems Committee,** chaired by M. Miles Matthews, Executive Officer, Counterdrug Intelligence Executive Secretariat.

- **Outreach Committee**, chaired by William Berger, Chief of the North Miami Beach, Florida, Police Department and past IACP president.

- **Training Committee**, chaired by Thomas O'Connor, Chief of the Maryland Heights, Missouri, Police Department.

Methodology

After the initial gathering in Atlanta, GIWG members convened two additional meetings to develop recommendations for the proposed National Criminal Intelligence Sharing Plan. The working environment of the GIWG Committees was issue-driven and recommendations were developed for each issue identified. This report will present the issues and recommendations formulated as a result of the GIWG Committees' discussions, deliberations, and collaborations.

Once the interim report is delivered, the working papers that were developed to support the issues and recommendations contained in the interim report will be presented to the entire membership of the GIWG for use during their upcoming meetings. Additionally, the interim report will be provided to various law enforcement groups so that feedback can be obtained on the broad recommendations.

The IACP *Criminal Intelligence Sharing Report* recommendations were utilized as a blueprint by the GIWG when developing recommendations for the proposed National Criminal Intelligence Sharing Plan. The GIWG focused their efforts on developing an intelligence gathering and sharing plan that emphasizes better methods for sharing among all agencies, and which describes a method for passing and receiving critical data among those agencies. Key to this process is the efficient leveraging of existing efforts—the commitment to build on, not re-invent, substantial information sharing activities already underway.

GIWG Mission Statement and Vision

A primary objective of the GIWG is to build on the existing intelligence sharing efforts by promoting intelligence-led policing through the development of the National Criminal Intelligence Sharing Plan. Intelligence-led policing is defined as *the collection and analysis of information to produce an intelligence end product designed to inform police decision making at both the tactical and strategic levels.* Intelligence-led policing is predicated on the production and application of intelligence information and products. For intelligence-led policing to be effective, the process must be an integral part of an agency's policies and strategies, and also integral in the organization's missions and goals. The GIWG members developed a mission statement to formalize their objective:

> *The GIWG mission is to develop, build, and support the creation of the National Criminal Intelligence Sharing Plan, which will provide justice-related agencies with the ability to gather, analyze, protect, and share information and intelligence to identify, investigate, prevent, deter, and defeat criminal and terrorist activities, both domestically and internationally, as well as protect the security of our homeland and preserve the rights and freedoms of all Americans.*

The GIWG membership also articulated a *vision* of what the National Criminal Intelligence Sharing Plan should be to local, state, tribal, and federal law enforcement agencies:

- *A model intelligence-sharing plan.*
- *A mechanism to provide seamless sharing of information between systems.*
- *A model for intelligence process principles and policies.*
- *A national model for intelligence training.*
- *An outreach model to promote intelligence sharing.*
- *A model for protecting individuals' privacy and civil rights.*
- *A blueprint for law enforcement administrators to follow when reviewing their own intelligence system or building a new one.*
- *A mechanism to promote intelligence-led policing.*

Issues and Recommendations

A goal of the GIWG is to assure that the guiding principles contained within the proposed National Criminal Intelligence Sharing Plan become institutionalized throughout the law enforcement community nationwide. The various components addressed by the Plan—system connections, personnel training, promulgation of model policies and standards, outreach efforts, and others—should be implemented in a multi-faceted and ongoing manner. The GIWG members envision that implementation of the Plan will provide the impetus for law enforcement agencies to institute intelligence–led policing, and doing so will help to substantially increase intelligence sharing and improve public safety. The following issues and recommendations are not presented by level of importance. *The recommendations should be considered tentative and may be modified in the final report.*

Issue 1: Identify an intelligence information sharing capability that can be accessed by local, state, tribal, and federal law enforcement and public safety agencies

As indicated in the IACP *Criminal Intelligence Sharing Report*, current capabilities to share criminal information and intelligence data are greatly disaggregated, although in the past year significant strides have been taken to connect these capabilities as a virtual system for state, local, tribal, and federal law enforcement, intelligence agencies, and first responder connectivity. IACP Summit participants and representatives of individual local, state, tribal, and federal law enforcement agencies noted that a considerable number of law enforcement and protective service organizations already engage in substantial information sharing. These efforts should be built upon, connected, and expanded, not replicated or kept static.

Recommendation 1: The Regional Information Sharing Systems (RISS) secure network (riss.net) and the Federal Bureau of Investigation's (FBI) Law Enforcement Online (LEO) system, which connected September 1, 2002, as a virtual system, should serve as the Sensitive but Unclassified (SBU) communications backbone for implementation of a nationwide intelligence sharing capability.

Recommendation 2: Information sharing utilizing the RISS/LEO communications capability should commence as soon as feasible, and existing systems at the local, state, regional, and national level should be integrated into the RISS/LEO communications capability in order to leverage information sharing. The GIWG conducted a preliminary survey of systems/initiatives currently operating at the local, state, federal, and regional level. Several systems/initiatives were identified. Refer to the appendix of this report for a list of the systems identified, as well as summary information obtained during the survey *(Appendix B).*

Recommendation 3: Intelligence sharing systems of a more regional or local scope that desire connection to the RISS/LEO communications capability should meet minimum requirements of being Web-enabled, Internet-based, capable of encrypted e-mail, authenticated to an individual user, and comported with the RISS/LEO security level.[4] Such systems should be encouraged to connect to the RISS/LEO communications capability, thereby expanding collaboration and

[4] Currently Triple-Data Encryption Standard (DES), though being enhanced to the National Institute of Standards and Technology (NIST) Advanced Encryption Standard (AES) in 2003.

information sharing opportunities and leveraging existing users. Moreover, system membership standards and vetting procedures must be compatible with those of the currently connected SBU systems, so as to be trusted connections to the nationwide RISS/LEO communications capability.

Recommendation 4: Agencies participating in the National Criminal Intelligence Sharing Plan are encouraged to use *Applying Security Practices to Justice Information Sharing, Models for Information Sharing, Volumes 1 and 2,* as reference documents regarding information system security practices. These documents are being developed to be used by justice executives and managers as a resource to secure their justice information systems and as a resource of ideas and best practices to consider when building their agency's information infrastructure and before sharing information with other agencies. These documents are in draft stage and are scheduled for completion in August 2003, and will be included in the October 2003 final report to BJA.

Recommendation 5: Agencies connecting databases and other resources to the RISS and LEO criminal intelligence sharing capabilities shall be encouraged to utilize the latest version of the Justice Extensible Markup Language Data Model[5]. The Data Model and its component Data Dictionary were developed to enable interoperability through the exchange of data across a broad range of disparate information systems. Almost all major software vendors fully support the general XML standard.

Recommendation 6: To ensure that trusted relationships are fostered, law enforcement agencies should require, support, and conduct background checks on individuals desiring law enforcement access to the RISS and LEO communications capability. Background requirements for access to the nationwide RISS/LEO communications capability by law enforcement personnel (sworn officers/agents and intelligence/crime analysts) shall be consistent with requirements applied to the designation and employment of sworn personnel, as set by the participating state, so long as, at a minimum, those requirements stipulate an FBI and state fingerprint-based records check. Further, that a fingerprint-based records check must have been completed within the previous three years.

Recommendation 7: The GIWG, in conjunction with BJA and the connected SBU systems, shall develop an acquisition mechanism or centralized site that will enable law enforcement agencies to access shared data visualization and analytic tools. The GIWG shall identify a standard "tool set" of analytical products that are recommended for use by law enforcement agencies in order to maximize resources when performing intelligence functions. The "tool set" may include, but not be limited to: search engines, data mining, link analysis, and geospatial mapping tools, as well as a resource list of current users of the products.

Issue 2: Overcome the longstanding and substantial barriers that hinder intelligence sharing

The IACP Criminal Intelligence Sharing Summit participants identified the following obstacles as some of the most significant hindering intelligence sharing: the absence of a nationally coordinated process for intelligence generation and sharing; the "hierarchy" within the

[5] The latest version of the Justice Extensible Markup Language (XML) Data Dictionary can be found at: http://www.it.ojp.gov/jxdm.

law enforcement and intelligence communities; local, state, tribal, and federal laws and policies that prevent sharing; the inaccessibility and/or disaggregation of technologies to support intelligence sharing; and deficits in analysis.

The Major Cities Chiefs Association recently sponsored a survey in which they requested survey respondents to provide the top five impediments to the flow of intelligence information between law enforcement agencies. Preliminary findings suggested that the results are consistent with the barriers identified by the Summit participants.

Recommendation 8: The GIWG shall develop a national Plan that promotes intelligence sharing and identifies mechanisms for resolving the barriers that hinder the exchange of intelligence. Some of the key elements of the Plan that will assist in eliminating barriers include: access to a nationwide network with links to local, state, federal, and regional databases; implementation of security requirements that institute trust in network participants; comprehensive training provisions and outreach mechanisms, both of which provide education and continued emphasis on intelligence sharing; availability of model policies and standards for all law enforcement agencies to emulate; and access to analytic resources and tools previously unavailable.

Issue 3: Increase availability of information from classified systems to state and local law enforcement agencies for the prevention and investigation of crime in their jurisdictions

The IACP *Criminal Intelligence Sharing Report* noted the difficulties of intelligence sharing between local, state, and federal law enforcement agencies. The current laws that guide the classification of intelligence information and individuals' clearance to view data are one example. The fact that some information needs to be classified is not disputed; however, the current process utilized needs to become more efficient to better serve public safety and homeland defense.

Recommendation 9: The GIWG, in conjunction with federal officials, should identify technical means to be used to produce unclassified, redacted tear-line[6] reports of classified data, excising sensitive source and method-of-collection data, yet retaining intelligence content, as much as feasible. To that end, three approaches are recommended: 1) utilize "reports" officers/analysts establishing a capability to generate and disseminate sanitized reports of current law enforcement investigative information to their counterpart law enforcement agencies at the local, state, and federal levels, 2) establish procedures and designate supervisory individuals to pass and receive sensitive "tips and leads," and 3) eliminate method-of-collection and source information from the report being shared.

Recommendation 10: Federal funds should be appropriated for more local and state law enforcement personnel to receive national security clearances, and the requisite background investigations should be funded so as to be performed more rapidly. The GIWG recognizes and appreciates the necessity of national security classification requirements. The GIWG realizes

[6] The definition of tear-line is a classified report that has information redacted from its content, primarily relating to the source of the data and method of collection.

that sharing such data requires that recipients must first have the requisite national security clearances. To that end, the GIWG recommends that federal funds be appropriated to permit federal background clearances to be performed and adjudicated in greater quantity and with greater speed than is currently experienced so local and state law enforcement personnel, with a need-to-know classified information, receive that information.

Issue 4: Ensure that individuals' constitutional rights, including civil liberties, civil rights, and privacy interests, are protected at every step of the intelligence process

The protection of individuals' privacy and constitutional rights is an obligation of government officials and is crucial to the long-term existence and success of criminal intelligence sharing. Protecting the privacy and constitutional rights of individuals, while at the same time providing for homeland security and public safety, will require a commitment from everyone in the system—from line officers to top management. Ensuring the protection of individuals' privacy and constitutional rights will be woven into all aspects of the proposed National Criminal Intelligence Sharing Plan, including the Plan's model policies and standards.

Recommendation 11: All parties involved with implementing and promoting the National Criminal Intelligence Sharing Plan should take steps to assure that the law enforcement community recognizes the importance of protecting individuals' privacy and constitutional rights within the intelligence process.

Recommendation 12: To further enhance professional judgment, especially as it relates to the protection of individuals' privacy and constitutional rights, the National Criminal Intelligence Sharing Plan should include provisions for encouraging participation in professional criminal intelligence organizations and supporting intelligence training for all law enforcement employees.

Recommendation 13: To foster trust between law enforcement agencies and their communities, the National Criminal Intelligence Sharing Plan should adopt a policy of openness regarding the criminal intelligence function (when it does not affect the security and integrity of the process).

Recommendation 14: The GIWG shall ensure that the proposed National Criminal Intelligence Sharing Plan identifies effective accountability measures that law enforcement agencies should utilize, to foster and ensure protection of individuals' privacy and constitutional rights, and to identify and remedy practices that are inconsistent with policy. Suggested accountability measures include: periodic reviews by management on decision making throughout the intelligence process; audit trails within intelligence processes and computer systems; staff surveys and questionnaires; effective training on department policies, procedures, and professional criminal intelligence practices; and periodic audits of criminal intelligence operations and files.

Recommendation 15: Law enforcement agencies involved in criminal intelligence sharing shall be encouraged to utilize, to the extent applicable, the privacy policy guidelines provided in *Justice Information Privacy Guideline – Developing, Drafting and Assessing Privacy Policy for*

Justice Information Systems.[7] The goal of the *Justice Information Privacy Guideline* is to provide assistance to justice leaders and practitioners who seek to balance public safety, public access, and privacy, when developing information policies for their individual agencies' or for integrated (multi-agency) justice systems.

Issue 5: Development of minimum standards for all levels of the intelligence process: Collection, Collation, Analysis/Evaluation, Storage/Retention, and Dissemination

The IACP Summit participants outlined several mandates to be addressed by the developers of the National Criminal Intelligence Sharing Plan, including the importance of ensuring compatible policies and standards for all levels of the intelligence process. The basics of intelligence are collection, collation, analysis, evaluation, storage/retention, and dissemination. The proper completion of these steps ensures that the data used are managed appropriately and within the legal constraints regarding privacy and the rights of all citizens.[8]

Recommendation 16: Law enforcement agencies should adopt the minimum standards required by federal regulation 28 CFR Part 23 for ensuring that the collection, access, storage, and dissemination of criminal intelligence conforms to the privacy and constitutional rights of individuals and groups and organizations, and also ensure that appropriate sharing of criminal intelligence between all levels of government – local, state, tribal, and federal – be facilitated, regardless of whether or not an intelligence system is federally funded.

Recommendation 17: Law enforcement agencies should consider the IACP's Criminal Intelligence Model Policy, with appropriate changes included, as a guide when implementing the National Criminal Intelligence Sharing Plan. (The revised Model Policy is included in *Appendix C.*) The purpose of the Model Policy is to provide law enforcement officers, in general, and officers assigned to the intelligence function, in particular, with guidelines and principles for the collection, analysis, and distribution of intelligence information. The GIWG, with concurrence from the National Law Enforcement Policy Center, suggested revisions to the Criminal Intelligence Model Policy to incorporate the recent proposed changes to 28 CFR Part 23.

Recommendation 18: In addition to federal regulation 28 CFR Part 23, law enforcement agencies should utilize the Law Enforcement Intelligence Unit (LEIU) Criminal Intelligence File Guidelines as an additional model for intelligence file maintenance. The March 2002 update of the LEIU Criminal Intelligence File Guidelines is attached as *Appendix D* to this report.

Issue 6: Development of minimum standards for management of an intelligence unit

In the aftermath of the 9/11 terrorist events, law enforcement agencies realize that they need to develop new capabilities and methods of deterring crime and terrorist activities, and more importantly, they need to share all—not just terrorism-related—criminal intelligence. The effective use of a criminal intelligence unit is crucial to a law enforcement agency's ability to combat crime. A properly managed criminal intelligence function can have a tremendous impact on a law enforcement agency and the community it serves.

[7] This document is available at: http://www.ncja.org/pdf/privacyguideline.pdf.

[8] *Intelligence 2000: Revising the Basic Elements*, p. 11.

Recommendation 19: Law enforcement agencies should adopt the minimum standards for management of an intelligence unit as outlined in the proposed National Criminal Intelligence Sharing Plan. The standards focus on the intelligence process and include elements such as: mission of the unit, management and supervision, personnel selection, training, security, privacy rights, promotion of intelligence products, and accountability measures.

Issue 7: Development of minimum training standards for all affected levels of law enforcement personnel to include training objectives, core curriculum, number of hours, and frequency of training

The IACP *Criminal Intelligence Sharing Report* included the recommendation to "promote intelligence-led policing through a common understanding of criminal intelligence and its usefulness." Standards for training on intelligence functions are critical to implementing a national model for intelligence-led policing. National intelligence training standards can provide criminal justice agencies, individually and collectively, with the framework for achieving that end. The goal of the training is to professionalize and enhance the practice of criminal intelligence collection within the United States law enforcement/criminal justice community, demonstrate the benefits derived from the intelligence, and encourage information sharing in support of the intelligence.

Recommendation 20: Training should be provided to all levels of law enforcement officials involved in the criminal intelligence process. The training standards, as contained within the National Criminal Intelligence Sharing Plan, should be considered the minimum training standards for all affected personnel. The recommended training standards for each level, including roles and missions, core training objectives, and length of training, are attached as *Appendix E* to this report. Additionally, recipients of criminal intelligence training, as recommended in the National Criminal Intelligence Sharing Plan, should be recognized and awarded certificates for successful completion of training.

Recommendation 21: The GIWG should foster a working relationship with the International Association of Directors of Law Enforcement Standards and Training (IADLEST) organization, the State and Provincial Police Academy Directors Section (SPPADS) of the IACP, and other appropriate training organizations in order to obtain their assistance with implementing the recommended National Criminal Intelligence Sharing Plan training standards in every state.

Issue 8: Ensure institutionalization of the National Criminal Intelligence Sharing Plan

As indicated in the IACP *Criminal Intelligence Sharing Report*, local, state, tribal, and federal law enforcement agencies, and the organizations that represent them, must all work together toward a common goal—gathering information and producing intelligence within their agency and sharing that intelligence with other law enforcement agencies. The sharing of timely, accurate, and complete information among justice-related agencies is critical to the defense of the United States and all Americans, at home and abroad. Getting credible and reliable intelligence to the agency in need is imperative to address criminal and terrorist activities. Whether it be the officer on the street, the intelligence manager, or the agency executive—having the information, which will help them do the job, is essential. The proposed National Criminal

Intelligence Sharing Plan should be a comprehensive, easily understood reference document that all law enforcement officers can access when desiring to implement or enhance the intelligence process in his or her organization.

Recommendation 22: The GIWG Outreach Plan *(Appendix F)* should be utilized to publicize and, more importantly, institutionalize the concepts of standards-based intelligence sharing and intelligence-led policing, as contained in the proposed National Criminal Intelligence Sharing Plan. The GIWG article and brochure, *Developing a National Criminal Intelligence Plan*, were developed as products of the GIWG Outreach Plan and are attached as *Appendix G.*

Recommendation 23: A National Signing Day should be held where law enforcement leaders and other relevant groups come together for a symbolic "sign-on" to the National Criminal Intelligence Sharing Plan. Participants on the National Signing Day should include a wide-range of law enforcement representatives from every level of government.

Recommendation 24: The GIWG should monitor the implementation of the National Criminal Intelligence Sharing Plan in order to gauge success of the Plan. Areas to evaluate should include community knowledge of the Plan, training efforts, agency adoption of policies and standards, and systems participating in the RISS/LEO nationwide communications capability. Assessment of the various components of the National Criminal Intelligence Sharing Plan should occur at different phases of its implementation in order to measure success of the project. Consideration should also be given to developing performance measures to gauge the results and outcomes of the Plan.

Issue 9: Develop a coordinating council that will provide and promote a coordinated, locally driven criminal intelligence generation and sharing process

The most central and enduring element of the National Criminal Intelligence Sharing Plan advocated by the IACP Summit participants is the call for a Criminal Intelligence Coordinating Council. The Summit participants viewed the Council as an ongoing solution to the need for a nationally coordinated, but locally driven, criminal intelligence generation and sharing process for the promotion of public safety.[9]

Recommendation 25: The GIWG should evolve into a Coordinating Council as contemplated in the IACP *Criminal Intelligence Sharing Report.* The GIWG membership recommends that a coordinating council be established to provide long-term oversight and assistance with implementation of the National Criminal Intelligence Sharing Plan. Several of the GIWG committees discussed this issue at length and all had differing opinions regarding the proposed council's membership, responsibilities, and authority. A final recommendation will be determined during the upcoming GIWG meetings and presented in the final report.

[9] IACP *Criminal Intelligence Sharing Report*, p. 2

Glossary

Administrative Analysis – The provision of economic, geographic, or social information to administrators. (Gottlieb, Singh, and Arenberg, 1995, p. 13)

Analysis (law enforcement) – The review of information and its comparison to other information to determine the meaning of the data in reference to a criminal investigation or assessment. (Peterson, 1994, p. 269)

Collation – The process whereby information is stored and cross-referenced so that it can be retrieved easily. (INTERPOL, 1996, p. 10)

Collection – The directed, focused gathering of information from all available sources. (INTERPOL, 1996, p. 9)

Collection Plan – The preliminary step toward completing a strategic assessment which shows what needs to be collected, how it is going to be collected, and by what date. (Peterson, 1994, p. 36)

Confidential – Information obtained through intelligence unit channels that is not classified as sensitive and is for law enforcement use only.

Counter Intelligence – Information compiled, analyzed, and/or disseminated in an effort to investigate espionage, sedition, subversion, etc., related to national security concerns.

Crime Analysis – A set of systematic, analytical processes directed at providing timely and pertinent information relative to crime patterns and trend correlations to assist operational and administrative personnel in planning in the deployment of resources for the prevention and suppression of criminal activities, aiding the investigative process, and increasing apprehensions and the clearances of cases. (Gottlieb, Singh, and Arenberg, 1995, p. 13)

Crime Pattern Analysis – Examining the nature, extent, and development of crime in a geographical area and a certain period of time. (Europol, 2000, insert 3)

Criminal Analysis – The application of analytical methods and products to data within the criminal justice field. (Peterson, 1994, p. 2)

Criminal Intelligence – Information compiled, analyzed, and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity.

Criminal Investigative Analysis – The use of components of a crime and/or the physical and psychological attributes of a criminal to ascertain the identity of the criminal. (Peterson, 1994, p. 42)

Data Owner – Agency or analyst that originally enters information or intelligence into a system.

Data Element – A field within a database that describes or defines a specific characteristic or attribute.

Descriptive Analysis – Data and information systematically organized, analyzed, and presented. (Europol, 2000, insert 3)

Dissemination – The release of information, usually under certain protocols. (Peterson, 1994, p. 271)

Evaluation – An assessment of the reliability of the source and accuracy of the raw data. (Morris and Frost, 1983, p. 4)

Explanatory Analysis – Analysis that attempts to understand the causes of criminality. It often includes the study of a large amount of variables and an understanding of how they are related to each other. (Europol, 2000, insert 3)

Feedback/Re-Evaluation – Reviews the operation of the intelligence process and the value of the output to the consumer. (Harris, 1976, p. 133)

Forecasting - The process which predicts the future on the basis of past trends, current trends, and/or future speculation. (Peterson, 1994, p. 46)

Indicator – Detectable actions and publicly available information revealing critical information. (Krizan, 1999, p. 63)

Inference Development – Drawing conclusions based on facts. (Peterson, 1994, p. 48)

Information Classification – Protects sources, investigations, and the individual's right to privacy and includes levels: sensitive, confidential restricted, and unclassified. (LEIU File Guidelines, as printed in Peterson, Morehouse, and Wright, 2001, p. 206)

Intelligence – The product of systematic gathering, evaluation, and synthesis of raw data on individuals or activities suspected of being, or known to be, criminal in nature. (Quoted in IACP, 1985, p. 5, from National Advisory Committee on Criminal Justice Standards and Goals, *Organized Crime,* 1976, p. 122). Intelligence is information that has been analyzed to determine its meaning and relevance. Information compiled, analyzed, and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity. (IACP National Law Enforcement Policy Center, 1998)

Intelligence Cycle – Planning and direction, collection, processing and collating, analysis and production, dissemination. (Morehouse, 2001, p. 8)

Intelligence Files – Stored information on the activities and associations of individuals, organizations, businesses, and groups who are suspected of being or having been involved in the actual or attempted planning, organizing, financing, or commission of criminal acts; or are suspected of being or having been involved in criminal activities with known or suspected crime figures. (LEIU Guidelines, in Peterson, Morehouse, and Wright, 2001, p. 202)

Intelligence-led Policing – The collection and analysis of information to produce an intelligence end product designed to inform police decision-making at both the tactical and strategic levels. (Smith, 1997, p. 1)

Investigative Information – Information obtained from a variety of sources – public, governmental, confidential, etc. The information may be utilized to further an investigation or could be derived from an investigation.

Need-to-Know – An individual requesting access to criminal intelligence data has the need to obtain the data in order to execute official responsibilities.

Network – A structure or system of connecting components designed to function in a specific way.

Operational Analysis – Identifying the salient features such as groups of or individual criminals, relevant premises, contact points, and methods of communication. (Europol, 2000, insert 3)

Operational Intelligence – Intelligence that details patterns, modus operandi, and vulnerabilities of criminal organizations but is not tactical in nature. (Morris and Frost, 1983, p. vi)

Operations Analysis – The analytic study of police service delivery problems, undertaken to provide commanders and police managers with a scientific basis for a decision or action to improve operations or deployment of resources. (Gottlieb, Singh, and Arenberg, 1995, p. 34)

Pointer Index – A listing within a database containing particular items that serve to guide, point out, or otherwise provide a reference to more detailed information.

Predictive Analysis – Using either descriptive or explanatory analytical results to reduce uncertainties and make an "educated guess." (Europol, 2000, insert 3)

Preventive Intelligence – Product of proactive intelligence. (Morris and Frost, 1983, p.6)

Privacy – An individual's interests in preventing the inappropriate collection, use, and release of personally identifiable information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data.

Problem Profile – Identifies established and emerging crime or incident series. (NCIS, 2001, p. 18)

Procedural Guidelines – Every criminal justice agency should establish procedural guidelines designed to provide a basic and general description for the collection of intelligence data. The guidelines should take into consideration the rights of privacy and any other constitutional guarantees. (IACP, 1985, p. 6)

Proactive – Obtaining data regarding criminal conspiracies in order to anticipate problems and forestall the commission of crimes. (Morris and Frost, 1983, p. 6)

Reasonable Indication – The reasonable indication threshold for collecting criminal intelligence is substantially lower than probable cause. A reasonable indication may exist where there is not yet a current substantive or preparatory crime, but where facts or circumstances reasonably indicate that such a crime will occur in the future.

Reasonable Suspicion – When information exists which establishes sufficient fact to give a trained law enforcement employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise. (Criminal Intelligence System Operating Policies, as printed in Peterson, Morehouse, and Wright, 2001, p. 212)

Recommendations – Suggestions for action to be taken by law enforcement management as a result of an analysis. (Peterson, 1994, p. 275)

Requirements – Validated and prioritized statements of consumers' needs for intelligence information. (Morris and Frost, 1983, vi)

Restricted Data –Reports, which at an earlier date, were classified sensitive or confidential and the need for high-level security no longer exists.

Right-to-know – An individual requesting access to criminal intelligence data has the right to access due to legal authority to obtain the information pursuant to a court order, statute, or decisional law.

Risk Assessment – A report aimed at identifying and examining vulnerable areas of the society that are, or could be, exploited. (Europol, 2000, insert 3) (Also see Vulnerability Assessment.)

Security – A series of procedures and measures which, when combined, provide protection of people from harm; information from improper disclosure or alteration; and, assets from theft or damage. (Criminal Justice Commission, 1995, as reprinted in Intelligence 2000: Revising the Basic Elements, p. 159)

Sensitive Data – Information pertaining to significant law enforcement cases currently under investigation and criminal intelligence reports that require strict dissemination and release criteria.

Situation Report – A mainly descriptive report that is oriented only towards the current crime situation. (Europol, 2000, insert 3)

Strategic Assessment – A long-term, high-level look at the law enforcement issues, which not only considers current activities but also tries to provide a forecast of likely developments. (NCIS, 2001, p. 17)

Strategic Intelligence – Most often related to the structure and movement of organized criminal elements, patterns of criminal activity, activities of criminal elements, projecting criminal trends, or projective planning. (IACP, 1985, p. 6, quoting National Advisory Committee, 1976, p. 122)

System – A group of databases that interact and form a whole structure.

Tactical Assessment – Ability to identify emerging patterns and trends requiring attention, including further analysis. (NCIS, 2000, p. 17)

Tactical Intelligence – Information regarding a specific criminal event that can be used immediately by operational units to further a criminal investigation, plan tactical operations, and provide for officer safety. (IACP, 1998, as reprinted in Peterson, Morehouse, and Wright, 2001, p. 218)

Target Profile – A profile that is person-specific and contains sufficient detail to initiate a target operation or support an ongoing operation against an individual or networked group of individuals. (NCIS, 2001, p. 18

Tear-Line Report – A classified report that has information redacted from its content, primarily relating to the source of the data and method of collection.

Threat Assessment – A strategic document, which looks at a group's propensity for violence or criminality, or the possible occurrence of a criminal activity in a certain time or place. (Peterson, 1994, pp. 56-57)

Unclassified Data – Civic-related information to which, in its original form, the general public had direct access (i.e., birth and death certificates). This would also include newspaper, magazine, and periodical clippings.

Vet – To subject to an expert appraisal or examine and evaluate for correctness.

Vulnerability Assessment – A strategic document which views the weaknesses in a system that might be exploited by a criminal endeavor.

Warning – A tactical warning is a very short-term warning that attack is either under way or so imminent that the forces are in motion or cannot be called back. A strategic warning is any type of warning or judgment issued early enough to permit decision makers to undertake countermeasures....ideally such warning may enable (them) to take measures to forestall the threat altogether. (Grabo, 1987, p. 6)

Appendix A

GIWG Membership and Acknowledgement Lists

GIWG Members

Mr. William Berger
North Miami Beach, Florida, Police Department
Miami, Florida

Mr. Donald Brackman
National White Collar Crime Center
Richmond, Virginia

Ms. Ledra Brady
U.S. Drug Enforcement Administration
Quantico, Virginia

Mr. Ron Brooks
Northern California HIDTA
San Francisco, California

Mr. Alan Carlson
The Justice Management Institute
Kensington, California

Mr. Melvin Carraway
Indiana State Police
Indianapolis, Indiana

Mr. Henry Coffman
INTERPOL-USNCB
Washington, DC

Mr. Carlo Cudio
Monterey, California, Police Department
Monterey, California

Mr. Michael Duffy
U.S. Department of Justice
Washington, DC

Mr. Thomas Frazier
Major Cities Chiefs Association
Baltimore, Maryland

Mr. Dennis Garrett
Arizona Department of Public Safety
Phoenix, Arizona

Mr. Vernon Keenan
Georgia Bureau of Investigation
Decatur, Georgia

Mr. Phil Keith
Knoxville, Tennessee, Police Department
Knoxville, Tennessee

Mr. Gerard P. Lynch
MAGLOCLEN
Newtown, Pennsylvania

Mr. George P. March
Regional Information Sharing Systems
Thorndale, Pennsylvania

Mr. Ritchie Martinez
Arizona Department of Public Safety/HIDTA
Tucson, Arizona

Mr. Jerry Marynik
California Department of Justice
Sacramento, California

Mr. Miles Matthews
Counterdrug Intelligence Executive Secretariat
U.S. Department of Justice
Washington, DC

Mr. Kent Mawyer
Texas Department of Public Safety
Austin, Texas

Mr. Peter Modafferi
Rockland County, New York, District Attorney's Office
New City, New York

Mr. Dennis Morton
U.S. Drug Enforcement Administration
Arlington, Virginia

Mr. John O'Nan
Ohio Office of the Attorney General
London, Ohio

Mr. Daniel Oates
Ann Arbor, Michigan, Police Department
Ann Arbor, Michigan

Mr. Thomas O'Connor
*Maryland Heights, Missouri,
Police Department
Maryland Heights, Missouri*

Ms. Marilyn Peterson
*New Jersey Division of Criminal
Justice
Trenton, New Jersey*

Mr. Russ Porter
*Iowa Department of Public Safety
Des Moines, Iowa*

Mr. Louis Quijas
*Federal Bureau of Investigation
Washington, DC*

Mr. Philip Ramer
*Florida Department of Law
Enforcement
Tallahassee, Florida*

Mr. Richard Randall
*Kendall County, Illinois,
Sheriff's Office
Yorkville, Illinois*

Mr. Steven Raubenolt
*Ohio State Highway Patrol
Columbus, Ohio*

Mr. Edward Reina
*Yavapai-Prescott Tribal Police
Department
Prescott, Arizona*

Mr. Jim Savage
*U.S. Department of Homeland
Security
Washington, DC*

Mr. Michael Schrunk
*Multnomah County District
Attorney's Office
Portland, Oregon*

Mr. Richard Stanek
*Minnesota Department of Public
Safety
St. Paul, Minnesota*

Mr. Gregory Stieber
*U.S. Department of Homeland
Security
Washington, DC*

Mr. Richard H. Ward III
*Bureau of Justice Assistance
Washington, DC*

Acknowledgements

The Global Intelligence Working Group wishes to acknowledge the following individuals for their contributions towards this interim report:

Mr. David Clopton
System Planning Corporation
Arlington, Virginia

Mr. Bruce Edwards
Bureau of Justice Assistance
Washington, DC

Mr. Bill Eubanks
Federal Bureau of Investigation (retired)
Washington, DC

Mr. Max Fratoddi
Federal Bureau of Investigation
Washington, DC

Mr. Steven Hooks
Federal Bureau of Investigation
Clarksburg, West Virginia

Mr. William Luechkenhoff
Federal Bureau of Investigation
Clarksburg, West Virginia

Mr. Allyn Lynd
Federal Bureau of Investigation
Clarksburg, West Virginia

Mr. Steve McGraw
Federal Bureau of Investigation
Washington, DC

Ms. Marilynn Nolan
U.S. Drug Enforcement Administration
Arlington, Virginia

Mr. Henry Pino
Ak-Chin Tribal Police Department
Maricopa, Arizona

Mr. Paul Redmond
U.S. Department of Homeland Security
Washington, DC

Mr. Neal Riddle
U.S. Department of Homeland Security
Washington, DC

Mr. Carl Ringwald
New York City, New York, Police Department
New York, New York

Mr. John Smith
U.S. Drug Enforcement Administration
Alexandria, Virginia

Ms. Lynn Starling
Federal Bureau of Investigation
Washington, DC

Mr. David Walchak
Federal Bureau of Investigation
Washington, DC

Appendix B

GIWG Information/Intelligence Sharing System Survey Overview and Survey Recap

Global Intelligence Working Group
Information/Intelligence Sharing System Survey

Background

At the February 2003, meeting of the Global Intelligence Working Group in San Francisco, California, detailed survey results were presented regarding 50 state intelligence systems. In addition, an overview was presented of around 30 possible multistate or interstate information sharing systems.

The information below was derived from a follow-up survey of the multistate or interstate systems/initiatives. Staff was unable to obtain information on all 30 of the original systems identified. Additionally, it became clear that some of the original systems identified were not electronic information sharing systems, nor did all the systems contain intelligence information. The list below was supplemented with a few state and local systems for comparison purposes.

Overview

Information was reported on 22 systems/initiatives:

- Nine interstate
- Six state systems
- Three city or county regional systems
- Four reported but did not fit the electronic system criteria

General observations:

- Numerous systems seem to be designing their system architecture for purposes of expansion beyond initial stages to connect or interface with other systems.
- Several systems cover significant population areas, even though they are not national systems.
- Around half of the systems do not currently contain intelligence information.
- Some of the systems are messaging systems but have the possibility for electronic intelligence sharing.
- Riss.net is connecting to several of the other systems: CISAnet, HIDTA, LEIU, LEO, MATRIX, and NLETS.
- Information was obtained on most major systems of interest, but not all (missing: JRIES (CATIC) and Joint Terrorism Task Force Information Sharing Initiative (Gateway)).

Systems/Initiatives

CDU-Houston:	Community Defense Unit – Houston, Texas, Police Department
CISAnet:	Criminal Information Sharing Network (Southwest Border States Anti-Drug Information System)
CLEAR-Chicago:	Citizen Law Enforcement Analysis and Reporting – Chicago, Illinois, area
COPLINK:	COPLINK
CriMNet-MN:	CriMNet Minnesota
EFSIAC:	Emergency Fire Services Information and Analysis Center
EPIC:	El Paso Intelligence Center
ERN-Dallas:	Emergency Response Network – Dallas, Texas, FBI
HIDTA:	High Intensity Drug Trafficking Areas
JNET-PA:	Pennsylvania Justice Network
LEIU:	Law Enforcement Intelligence Unit
LEO:	Law Enforcement Online
LETS-AL:	Law Enforcement Tactical System – Alabama
MATRIX:	Multistate Anti-Terrorism Information Exchange
NLETS:	National Law Enforcement Telecommunication System
Project North Star:	Project North Star
RAID:	Real-time Analytical Intelligence Database
riss.net:	Regional Information Sharing Systems Secure Intranet
SIN-OK:	State Intelligence Network – Oklahoma
SPIN-CT:	Statewide Police Intelligence Network – Connecticut
TEW Group-Los Angeles	Terrorism Early Warning Group – Los Angeles, California area
ThreatNet-FL:	ThreatNet Florida

Summary Results

- Of the 22 systems, 14 were governed/controlled by host agencies and 12 by policy boards (there was some overlap). Policy board governance is especially popular among the larger systems.

- Sixteen of the 22 systems receive federal grants or appropriations as a source of funding for their system/initiative.

- Of the 22 systems, 8 were national in geographic service coverage, 7 regional, and 7 state-local.

- Of the 22 systems, 15 have federal agency members, 17 state members, 18 local members, and 13 other agency members.

- Seven were intrastate is the scope of geographic access for their system/initiative, 12 interstate, and 3 international.

- Twelve systems have law-enforcement-only agency access, and 10 law-enforcement-plus access.

- Thirteen systems contain general criminal data, 11 terrorism data, 11 drug data, and 9 gang data.

- Eight systems store system data at a central location, and 14 at decentralized locations.

- Nine systems own the data in the system, and 13 report that data contributors own the data.

- Eleven systems contain intelligence data and are 28 CFR Part 23-compliant.

- Means of connectivity include the following applications: VPN, intranet, extranet secure environment, firewall, Web-based, routers, and IP encrypted. Media used for connectivity include fiber, satellite, T-1, T-3, dial-up, and fractional (T-1).

- Nearly every system described itself as a limited access system (an invited community).

- Membership vetting methods include an application process, verification, screening, background checks, user certification training requirements, sponsorship, board approval, and member agency approval.

- User authentication methods include passwords, PKI, smart cards, tokens, key fobs, and digital certificates.

List of Systems/Initiatives

CDU-Houston:	Community Defense Unit – Houston, Texas, Police Department
CISAnet:	Criminal Information Sharing Network (Southwest Border States Anti-Drug Information System)
CLEAR-Chicago:	Citizen Law Enforcement Analysis and Reporting – Chicago, Illinois, area
COPLINK:	COPLINK
CriMNet-MN:	CriMNet Minnesota
EFSIAC:	Emergency Fire Services Information and Analysis Center
EPIC:	El Paso Intelligence Center
ERN-Dallas:	Emergency Response Network – Dallas, Texas, FBI
HIDTA:	High Intensity Drug Trafficking Areas
JNET-PA:	Pennsylvania Justice Network
LEIU:	Law Enforcement Intelligence Unit
LEO:	Law Enforcement Online
LETS-AL:	Law Enforcement Tactical System – Alabama
MATRIX:	Multistate Anti-Terrorism Information Exchange
NLETS:	National Law Enforcement Telecommunication System
Project North Star:	Project North Star
RAID:	Real-time Analytical Intelligence Database
riss.net:	Regional Information Sharing Systems Secure Intranet
SIN-OK:	State Intelligence Network – Oklahoma
SPIN-CT:	Statewide Police Intelligence Network - Connecticut
TEW Group-LA:	Terrorism Early Warning Group – Los Angeles
ThreatNet-FL:	ThreatNet Florida
TOTAL:	**22 Systems/Initiatives**

1) How is your system/initiative governed/controlled?

a. Host agency:

CDU-Houston	Houston Police Department
CLEAR-Chicago	Chicago Police Department
COPLINK	Phoenix Police Department
CriMNet	Not Centralized. CriMNet connects and manages architecture.
EFSIAC	U.S. Fire Administration
ERN-Dallas	FBI
HIDTA	Office of Drug Control Policy
LEO	FBI
Project North Star	U.S. Border Patrol
RAID	National Drug Intelligence Center
SIN-OK	OSBI
SPIN-CT	Connecticut State Police – Intelligence Unit
TEW Group-LA	Los Angeles Sheriff's Department
ThreatNet-FL	FDLE

b. **Policy board (makeup, current chair):**

CISAnet	CISA Board of Directors – Chair: Marshall Caskey
CriMNet	Criminal & Juvenile Justice Information Police Group – Chair: Richard Stanek
EPIC	Five federal agencies: DEA, FBI, USCG, Customs, and INS. The chair is always the DEA EPIC Director, currently Jim Mavromatis. The Deputy Director position at EPIC is rotated between the other agencies
HIDTA	Each HIDTA group has an Executive Board made up of equal numbers of federal, state, and local law enforcement members.
JNET-PA	Executive Council: Department of Corrections, State Police, Probation & Parole, Board of Pardons, Governor's Office, Administrator of Courts, Juvenile Courts, Public Welfare, Department of Transportation, Inspector General, Commission on Crime & Delinquency, and Office of the Budget. Chair: Fritz Bittenbender, Governor's Office of Administration.
LEIU	LEIU Executive Board (Chair Richard Wright of Simi Valley, California, CA PD); riss.net – RISS Directors Association Chair: Jerry Lynch of MAGLOCLEN
LETS-AL	Informal Policy Board made up of: the Attorney General's Office, the Administrative Office of Courts and the Southwest Alabama Integrated Criminal Justice System - Chair: Jim Pritchett
MATRIX	14-member Executive Committee – Chair: Commissioner Tim Moore of Florida Department of Law Enforcement
NLETS	Board of Directors – Chair: Larry Grund, Iowa Department of Public Safety
Project North Star	Project North Star is governed by a National Quad Chair leadership representing U.S. federal agencies, U.S. state and local agencies, Canadian federal agencies, and Canadian provincial/regional agencies
riss.net	RISS Directors National Policy Board (comprised of six RISS center directors and policy board chair of each center) Chair: Jerry Lynch of MAGLOCLEN
ThreatNet-FL	The Florida Domestic Security and Counter-Terrorism Intelligence Advisory Committee; comprised of (8) primary voting members, one representative appointed by each respective Regional Domestic Security Task Force Co-chairs, and the Chair to be appointed by the Domestic Security Oversight Committee

c. **Other:**

JNET-PA	JNET Senior Policy Team & the JNET Steering Committee
SPIN-CT	Commander of CSP Intel is Director

2) What are the sources of funding for your system/initiative?

System/Initiative	Federal Grant/Appropriations	State	Local	Other
CDU-Houston			X	
CISAnet	X	X		
CLEAR-Chicago	X (14 Million DOJ – COPS, Byrne, FBI)		X	X Programmers from Oracle ($10 Million)

System/Initiative	Federal Grant/Appropriations	State	Local	Other
COPLINK	X (NIJ)		X	
CriMNet	X (COPS)	X (Primary)		X Occasional Byrne Grants
EFSIAC	X (FEMA)			
EPIC	X (Federal: DEA Congressional Appropriation			
ERN-Dallas	X (Federal Homeland Security)			
HIDTA	X			
JNET-PA		X		
LEIU	X (for riss.net)			X Annual membership fee of $495
LEO	X			X (FBI)
LETS-AL	X (Appropriation)			
MATRIX	X			
NLETS				X 73 members pay annual fees of $25,200 each
Project North Star				Project North Star does not have any **system** in place. We are not an intelligence gathering organization, and we do not keep any files. As far as who funds Project North Star, everything is presently funded by the U.S. Border Patrol.
RAID	X (DOD)			
riss.net	X			
SIN-OK	X	X		X SIN recently received a $100,000 Byrne Grant for a computer upgrade
SPIN-CT	X			

System/Initiative	Federal Grant/Appropriations	State	Local	Other
TEW Group-LA				Participating Agencies – Los Angeles Sheriff's Department, LAPD, LA Fire Department, LA County Fire Department, LA Department of Health Services, LA Airport Police, and LA FBI.
ThreatNet-FL		X		
TOTAL	**16**	**5**	**3**	**6**

3) What is the service coverage area for your system/initiative?

System/Initiative	National	Federal	Regional	State-Local	Other
CDU-Houston			X (Connected to JRIES)		
CISAnet				X (CA, AZ, NM, TX, GA, ID)	
CLEAR-Chicago			X		
COPLINK			X		
CriMNet				X	
EFSIAC	X				
EPIC	X				
ERN-Dallas			X (Pilot project)		
HIDTA	X				
JNET-PA				X	
LEIU	X				
LEO	X				
LETS-AL			X		
MATRIX			X (Multistate region)		
NLETS	X				
Project North Star				X	
RAID	X				
riss.net	X				

System/Initiative	National	Federal	Regional	State-Local	Other
SIN-OK				X	
SPIN-CT				X	
TEW Group-LA			X (All of LA County)		
ThreatNet-FL				X	
TOTAL	**8**	**0**	**7**	**7**	**0**

4) What is the number of agencies and/or individual users for your system/initiative?

System/ Initiative	Federal Agencies		State Agencies		Local Agencies		Individuals		Other Agencies	
CISAnet	X	12	X	10	X	556	X	5,761	X	282
CLEAR-Chicago	X	3			X	132	X	20,000		
COPLINK					X	1				
CriMNet-MN			X		X				X	CJIS
EFSIAC									X	Approximately 32,000 Fire and EMS
EPIC	X	All (by their request)	X	50 (Some states have 2 or more users)	X	(As approved by the state rep.)				
ERN-Dallas	X	33	X	9	X	500+			X	30 Fire Departments, 25 Critical Infrastructures, 300 North Texas Corporations & Organizations, and All Military Branches
JNET-PA	X	12	X	39	X	County: 30 City Police: 200+			X	District Judges: 500
LEIU			X	54	X	172			X	Foreign – 6
LEO	X		X		X		X	40,000	X	
LETS-AL	X		X		X	350	X	2,000 users	X	CJIS
MATRIX			X	13						
NLETS	X	*	X	*	X	*				* 30,000 - Devices/ Terminals: 435,000
Project North Star	X	U.S. and Canadian	X		X	U.S.			X	Provincial/Regional agencies

System/ Initiative	Federal Agencies		State Agencies		Local Agencies		Individuals		Other Agencies	
RAID	X		X		X				X	International
riss.net	X		X		X		X	11,127	X	Federal, state, local, and other agencies connected: 3,432 Individual users at these agencies: 11,127
SIN-OK	X	6	X	8	X	51	X	194	X	Included in above: IRS, Austin, Texas, and Hemphill County, Texas, Sheriff's Office. There are 194 certified/trained users of the system. OSBI has 43 of the 194 users.
SPIN-CT	X	3	X	52 (Each state police location counted as one.)	X	50	X	950		
TEW Group-LA	X	15-20	X	6	X	100			X	Private Companies (critical infrastructure businesses), including major defense and intelligence companies.
ThreatNet-FL	X	*	X	*	X	*	X	476		*160 federal, state, and local agencies
TOTAL	**15**		**17**		**18**		**8**		**13**	

5) What is the scope of geographic access for your system/initiative?

System/Initiative	Intrastate	Interstate	Federal	International
CDU-Houston		X		
CISAnet		X		
CLEAR-Chicago	X (Talking to several out-of-state major city police departments reference connect, exchange, and share information. The State Law Enforcement Agencies Data Systems, Illinois LEADS, will be connected with CLEAR in 6/9 months.)			
COPLINK	X			
CriMNet		X		
EFSIAC		X		
EPIC				X
ERN-Dallas	X			
HIDTA		X		
JNET-PA	X			
LEIU		X		

System/Initiative	Intrastate	Interstate	Federal	International
LEO		X		
LETS-AL		X (Mississippi and Louisiana: Web-based)		
MATRIX		X		
NLETS				X
Project North Star				X
RAID		X		
riss.net		X		
SIN-OK		X		
SPIN-CT	X			
TEW Group-LA	X			
ThreatNet-FL	X			
TOTAL	**7**	**12**	**0**	**3**

6) What is the scope of agency access for your system/initiative?

System/Initiative	Law Enforcement Only	Law Enforcement Plus
CDU-Houston	X	
CISAnet	X	
CLEAR-Chicago		X
COPLINK	X	
CriMNet		X
EFSIAC		X (Fire and EMS)
EPIC	X	
ERN-Dallas		X
HIDTA	X	
JNET-PA		X
LEIU	X	
LEO		X
LETS-AL		X
MATRIX	X	
NLETS		X
Project North Star		X
RAID	X	

System/Initiative	Law Enforcement Only	Law Enforcement Plus
riss.net	X	
SIN-OK	X	
SPIN-CT	X	
TEW Group-LA		X
ThreatNet-FL	X	
TOTAL	**12**	**10**

7) What type of data is contained in your system/initiative?

System/ Initiative	General Criminal	Terrorism	Drugs	Gangs	Other
CDU-Houston		X			
CISAnet	X	X	X	X	X (Open source, investigative, seizure, etc.)
CLEAR-Chicago	X	X	X	X	X (CJIS, APHIS, 911 Call information)
COPLINK	X				X (All police department reports and other criminal justice information.)
CriMNet	X				X (Law enforcement contact information: traffic stops, complaints, accident victim, witness ECT) - CJIS Files
EFSIAC					X (Information relative to critical infrastructure particular to Fire and EMS)
EPIC			X		X (Guns, aliens, and any criminal predicate interest by a member agency.)
ERN-Dallas					X (Not a database system)
HIDTA	X	X	X	X	
JNET-PA	X				X (CJIS)
LEIU	X	X	X	X	X (High tech)
LEO	X	X	X	X	X (Bombs, hostage negotiators)
LETS-AL					X (CJIS)
MATRIX	X	X	X	X	
NLETS					X (N/A – information shared, not stored.)
Project North Star					X (Project North Star does not keep any files that can be construed as intelligence files. All material is for reference purposes only.)
RAID			X		X (Computer information/document information)
riss.net	X	X	X	X	
SIN-OK	X				
SPIN-CT	X	X	X	X	
TEW Group-LA	X	X	X	X	X (CJIS & Public Source Information)

System/ Initiative	General Criminal	Terrorism	Drugs	Gangs	Other
ThreatNet-FL		X			
TOTAL	13	11	11	9	14

8) Where is the system data located?

System/Initiative	A Central Location	Decentralized Locations
CDU-Houston		X
CISAnet		X
CLEAR-Chicago	X	
COPLINK		X
CriMNet		X
EFSIAC	X (Not a data system, Emergency Fire Services Information Sharing and Analysis Center (ISAC) is located in Emmitsburg, MD, at the U.S. Fire Administration Headquarters and Training Center. ISAC has a MOU/operating agreement with the National Infrastructure Protection Center (NPIC). It is a Web site and messaging service for Fire and EMS members nationwide.)	
EPIC		X (Six primary databases accessed by Multi-Database Query, MDBQ)
ERN-Dallas	X	
HIDTA		X (HIDTA Investigative Support Centers in each HIDTA Center)
JNET-PA		X
LEIU	X	
LEO	X	
LETS-AL		X
MATRIX		X
NLETS		X
Project North Star	X	

System/Initiative	A Central Location	Decentralized Locations
RAID		X (Not a data system, RAID is a tool, a software database program on CD-ROM that is distributed to local, state, and federal law enforcement agencies. NDIC also provides training in its use. It is a "linking" database for major cases. It is not an agency-to-agency shared database. The Document Exploitation Division of NDIC deploys teams of intelligence analysts to federal agency field offices or other sites to expedite the exploitation of information seized in major federal drug investigations. Document Exploitation teams use a state-of-the-art computer database developed at NDIC know as Real-time Analytical Intelligence Database (RAID) to quickly collect, collate, and label large volumes of information from seized documents and computers. The team then subjects this material to detailed analysis to help identify hidden assets, previously unknown associates, and other leads for further investigation.)
riss.net		X
SIN-OK	X	
SPIN-CT		X
TEW Group-LA		X (Multiple data systems – state, local, and federal)
ThreatNet-FL	X	
TOTAL	**8**	**14**

9) Who owns the data contained in your system/initiative?

System/Initiative	The System	Data Contributors
CDU-Houston	X	
CISAnet		X
CLEAR-Chicago	X	
COPLINK	X	
CriMNet		X
EFSIAC	X	
EPIC		X
ERN-Dallas	X	
HIDTA	X	
JNET-PA		X
LEIU		X
LEO		X

System/Initiative	The System	Data Contributors
LETS-AL	X (Read-only access to several data systems)	
MATRIX		X
NLETS		X
Project North Star	X	
RAID		X
riss.net		X
SIN-OK		X
SPIN-CT		X
TEW Group-LA	X	
ThreatNet-FL		X
TOTAL	**9**	**13**

10) What policies/standards does your system/initiative utilize for:

System/Initiative	Intelligence	Connectivity	Accessibility	User Authentication	Membership Vetting
CISAnet	28 CFR Part 23, state policies, CISA policies	Secure VPN, frame relay, fiber, satellite	Private system (a specific community)	Two-factor PKI authentication: smart cards, USB tokens, key fobs (roaming users), and standards-based digital certificates with vetted policies and procedures for certificate authorities and management, registration, global naming conventions, and certificate policies	The interested agency submits a letter of request to the appropriate Director. The agency is invited to attend a subsequent Directors' meeting where the mutual benefit of membership is discussed. Membership is approved by majority vote.
CLEAR-Chicago	28 CFR Part 23-Compliant	Intranet – Extranet Secure Environment	PC number identifier unique to each user	Password	Background on each user and successful completion of training for each user after acceptance
COPLINK	N/A	Internet Web-based browser with firewalls	Limited access	Internet with user ID and password	By user department

System/Initiative	Intelligence	Connectivity	Accessibility	User Authentication	Membership Vetting
CriMNet	Not an intelligence system	State system	Limited access	State system users ORI#. CriMNet is moving toward one user ID and password	DPS Policy – User organization authorization and ID profile
EFSIAC	N/A	Web site/NLETS	Limited access system	Name of department, name of chief and phone number	Spot checks
EPIC	28 CFR Part 23	Through EPIC Watch Commander	Limited access	Validation by user name, background, and individual particulars in EPIC system	State or federal member must sponsor; provide background
ERN-Dallas	N/A	Internet based – also NLETS, T-3 and Satellite through FEMA	Limited access		
HIDTA	28 CFR Part 23-Compliant	Limited access	RISS/HIDTA, VPN	Smart Card V-ONE technology same as RISS	Joint User – HIDTA has an Account Manager located with Riley Bell at RISS OIT. The Account Manager monitors HIDTA traffic/use to assure user authentication.
JNET-PA		Web-based Netscape Navigator, Microsoft Internet Explorer, and the JNET HTML framework	Limited access	Encryption, digital certificates, password	JNET user administration requirements
LEIU	LEIU Criminal Intelligence File Guidelines and 28 CFR Part 23	riss.net (secure VPN, frame relay, users via nodes (T-1), Internet, or dial-up access)		riss.net (smart card readers, smart cards, virtual tokens, passwords)	LEIU – application process, sponsorships; RISS – agency application process, screening, background checks, plus member agency individuals desiring access also must apply
LEO		Secure VPN, frame relay, users via nodes (T-1), Internet, or dial-up access	Limited access system (an invited community)	SmartPass, virtual tokens, passwords	Interested individuals apply and are screened

System/Initiative	Intelligence	Connectivity	Accessibility	User Authentication	Membership Vetting
LETS-AL	Not an Intelligence system	Web-based – digital	Limited access	VPN connections, User ID and password	Local agency head is validated. The agency head vouches for and validates their users.
MATRIX	28 CFR Part 23	Node connections on riss.net: secure VPN, frame relay, users via nodes (T-1), Internet, or dial-up access	Limited access (an invited community)	Smart card readers, smart cards, virtual tokens, passwords	RISS membership criteria (interested agencies apply and are screened, including a background check; member agency individuals desiring access must also apply) plus additional application criteria to access some intelligence information
NLETS	N/A	Fractional, T-1, frame, 128 KB minimum, routers, IP encrypted	Limited access system (an invited community)	Must be approved on the network that is controlled by each state	Must be approved for NCIC ORI number and complete application form
Project North Star	We do not keep intelligence files at Project North Star	We do not have anyone connecting to a system at this time	We have been developing a Newsletter and Web site but both are still being developed	Not in place	All members are identified through verification of agency credentials
RAID	N/A	N/A	Private System – Limited access system	N/A	N/A
riss.net	28 CFR Part 23	Secure VPN, frame relay, users via nodes (T-1), Internet, or dial-up access	Limited access system (an invited community)	Smart card readers, smart cards, virtual tokens, passwords	Interested agencies apply and are screened, including a background check. Member agency individuals desiring access also must apply.
SIN-OK	28 CFR Part 23 and written guidelines for users	Web-based	Limited access system	VPN Technology – Password	MOU agency submits user names, OSBI does background and user certification training
SPIN-CT	28 CFR Part 23	Dial-up modem and collect (state) data lines	Limited access system	Lotus notes, ID, and passwords	Access level determined by director, limited to law enforcement agencies

System/Initiative	Intelligence	Connectivity	Accessibility	User Authentication	Membership Vetting
TEW Group-LA	California and 28 CFR Part 23-Compliant			TEW Analysts – User ID	Based upon need and Individual database requirements
ThreatNet-FL	28 CFR Part 23, Sections 119.07 (3) (6), 119.011 (3), 119.072, and the operating guidelines	CJNet connectivity required	Limited access system (an invited community)	User name, password	Access to CJNet, activity involved in counter-terrorism activities, sign an agency agreement form, complete an updated agency security background check, complete an individual user agreement form, attend user training

Appendix C

Revised IACP Model Policy

IACP National Law Enforcement Policy Center
CRIMINAL INTELLIGENCE
Model Policy
February 1998, Revised June 2003

I. PURPOSE

It is the purpose of this policy to provide law enforcement officers in general, and officers assigned to the intelligence function in particular, with guidelines and principles for the collection, analysis, and distribution of intelligence information.

II. POLICY

Information gathering is a fundamental and essential element in the all-encompassing duties of any law enforcement agency. When acquired, information is used to prevent crime, pursue and apprehend offenders, and obtain evidence necessary for conviction. It is the policy of this agency to gather information directed toward specific individuals or organizations where there is a reasonable indication (as defined in 28 CFR, Part 23, Section 23.3 c) that said individuals or organizations may be planning or engaging in criminal activity, to gather it with due respect for the rights of those involved, and to disseminate it only to authorized individuals as defined. While criminal intelligence may be assigned to specific personnel within the agency, all members of this agency are responsible for reporting information that may help identify criminal conspirators and perpetrators.

Deleted:

Deleted: reasonably suspected of criminal activity.

The policy contained herein is intended to remain at all times consistent with the current language of 28 CFR, Part 23, as amended.

III. DEFINITIONS

Criminal Intelligence. Information compiled, analyzed and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity.

Strategic Intelligence. Information concerning existing patterns or emerging trends of criminal activity designed to assist in criminal apprehension and crime control strategies, for both short- and long-term investigative goals.

Tactical Intelligence. Information regarding a specific criminal event that can be used immediately by operational units to further a criminal investigation, plan tactical operations and provide for officer safety.

Threshold for criminal intelligence. The threshold for collecting information and producing criminal intelligence shall be the "reasonable indication" standard in 28 CFR, Part 23, Section 23.3 c, which reads: "reasonable indication means that an objective, factual basis for initiating an investigation exists. The standard of reasonable indication is substantially lower than probable cause. In determining if there is reasonable indication of criminal activity, a law enforcement officer may take into account any facts or circumstances that a prudent investigator would consider. The standard, however, requires specific facts or circumstances indicating a past, current, or future violation; a mere hunch is insufficient."

IV. PROCEDURES

A. Mission

It is the mission of the intelligence function to gather information from all sources in a manner consistent with the law, and to analyze that information to provide tactical and/or strategic, intelligence on the existence, identities, and capabilities of criminal suspects and enterprises generally and, in particular, to further crime prevention and enforcement objectives/priorities identified by this agency.

Deleted: in support of efforts

Deleted: information

1. Information gathering in support of the intelligence function is the responsibility of each member of this agency although specific assignments may be made as deemed necessary by the officer-in- charge (OIC) of the intelligence authority.
2. Information that implicates, suggests implication or complicity of any public official in criminal activity or corruption shall be immediately reported to this agency's chief executive officer or another appropriate agency.

B. Organization

Primary responsibility for the direction of intelligence operations; coordination of personnel; and collection, evaluation, collation, analysis, and dissemination of intelligence information is housed in this agency's intelligence authority under direction of the intelligence OIC.

1. The OIC shall report directly to this agency's chief executive officer or his designate in a manner and on a schedule prescribed by the chief.
2. To accomplish the goals of the intelligence function and conduct routine operations in an efficient and effective manner, the OIC shall ensure compliance with the policies, procedures, mission, and goals of the agency.

C. Professional Standards

The intelligence function is often confronted with the need to balance information-gathering requirements for law enforcement with the rights of individuals. To this end, members of this agency shall adhere to the following:

1. Information gathering for intelligence purposes shall be premised on circumstances that provide a reasonable indication (as defined in 28 CFR, Part 23, Section 23.3 c) that specific individuals or organizations may be planning or engaging in criminal activity.

Deleted: that a crime has been committed or is being planned.

2. Investigative techniques employed shall be lawful and only so intrusive as to gather sufficient information to prevent criminal conduct or the planning of criminal conduct.

Deleted: the criminal act and/or to identify and prosecute violators.

3. The intelligence function shall make every effort to ensure that information added to the criminal intelligence base is relevant to a current or on-going investigation and the product of dependable and trustworthy sources of

information. A record shall be kept of the source of all information received and maintained by the intelligence function.

4. Information gathered and maintained by this agency for intelligence purposes may be disseminated only to appropriate persons for legitimate law enforcement purposes in accordance with law and procedures established by this agency. A record shall be kept regarding the dissemination of all such information to persons within this or another law enforcement agency.

D. Compiling Intelligence

1. Intelligence investigations/files may be opened by the intelligence OIC with sufficient information and justification. This includes but is not limited to the following types of information.
   a. subject, victim(s) and complainant as appropriate; summary of suspected criminal activity;
   b. anticipated investigative steps to include proposed use of informants, photographic, or electronic surveillance;
   c. resource requirements, including personnel, equipment, buy/flash monies, travel costs, etc;
   d. anticipated results; and
   e. problems, restraints or conflicts of interest.
2. Officers shall not retain official intelligence documentation for personal reference or other purposes but shall submit such reports and information directly to the intelligence authority.
3. Information gathering using confidential informants as well as electronic, photographic, and related surveillance devices shall be performed in a legally accepted manner and in accordance with procedures established for their use by this agency.
4. All information designated for use by the intelligence authority shall be submitted on the designated report form and reviewed by the officer's immediate supervisor prior to submission.

E. Analysis

Formatted: Bullets and Numbering

1. Where possible, agencies involved in the intelligence function should establish and maintain a process to ensure that information gathered is subjected to review and analysis to derive its meaning and value.

Formatted: Bullets and Numbering

2. Where possible, the above-described process should be accomplished by professional, trained analysts.
3. Analytic material (i.e., intelligence) shall be compiled and provided to authorized recipients as soon as possible where meaningful trends, patterns, methods, characteristics or intentions of criminal enterprises or individuals emerge.

F. Receipt/Evaluation of Information

Upon receipt of information in any form, the OIC shall ensure that the following steps are taken:

1. Where possible, information shall be evaluated with respect to reliability of source and validity of content. While evaluation may not be precise, this assessment must be made to the degree possible in order to guide others in using the information. A record shall be kept of the source of all information where known.
2. Reports and other investigative material and information received by this agency shall remain the property of the originating agency, but may be retained by this agency. Such reports and other investigative material and information shall be maintained in confidence, and no access shall be given to another agency except with the consent of the originating agency.
3. Information having relevance to active cases or that requires immediate attention shall be forwarded to responsible investigative or other personnel as soon as possible.
4. Analytic material shall be compiled and provided to authorized sources as soon as possible where meaningful trends, patterns, methods, characteristics, or intentions of criminal enterprises or figures emerge.

G. File Status

Intelligence file status will be classified as either "open" or "closed," in accordance with the following:

1. Open

___Intelligence files that are actively being worked will be designated as "Open." in order to remain open, officers working such cases must file intelligence status reports covering case developments at least every 180 days.

2. Closed

___"Closed" intelligence files are those in which investigations have been completed, where all logical leads have been exhausted, or where no legitimate law enforcement interest is served. All closed files must include a final case summary report prepared by or with the authorization of the lead investigator

H. Classification/Security of Intelligence

1. Intelligence files will be classified in order to protect sources, investigations, and individual's rights to privacy, as well as to provide a structure that will enable this agency to control access to intelligence. These classifications shall be reevaluated whenever new information is added to an existing intelligence file.

   a. Restricted

   ___"Restricted" intelligence files include those that contain information that could adversely affect an on-going investigation, create safety hazards for officers, informants, or others and/or compromise their identities. Restricted intelligence may only be released by approval of the intelligence OIC or the agency chief executive to authorized law enforcement agencies with a need and a right to know.

   b. Confidential

____"Confidential" intelligence is less sensitive than restricted intelligence. It may be released to agency personnel when a need and a right to know has been established by the intelligence OIC or his designate.

c. Unclassified

____"Unclassified" intelligence contains information from the news media, public records, and other sources of a topical nature. Access is limited to officers conducting authorized investigations that necessitate this information.

2. All restricted and confidential files shall be secured, and access to all intelligence information shall be controlled and recorded by procedures established by the intelligence OIC.

   a. Informant files shall be maintained separately from intelligence files.

   b. Intelligence files shall be maintained in accordance with state and federal law.

   c. Release of intelligence information in general and electronic surveillance information and photographic intelligence, in particular, to any authorized law enforcement agency shall be made only with the express approval of the intelligence OIC and with the stipulation that such intelligence not be duplicated or otherwise disseminated without the approval of this agency's OIC.

   d. All files released under freedom of information provisions or through disclosure shall be carefully reviewed.

I. Auditing and Purging Files

1. The OIC is responsible for ensuring that files are maintained in accordance with the goals and objectives of the intelligence authority and include information that is both timely and relevant. To that end, all intelligence files shall be audited and purged on an annual basis as established by the agency OIC through an independent auditor.

2. When a file has no further information value and/or meets the criteria of any applicable law, it shall be destroyed. A record of purged files shall be maintained by the intelligence authority.

This project was supported by Grant No. 95-DD-BX-K014 awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. The Assistant Attorney General, Office of Justice Programs, coordinates the activities of the following program offices and bureaus: the Bureau of Justice Assistance, the Bureau of Justice Statistics, National Institute of Justice, Office of Juvenile Justice and Delinquency Prevention, and the Office of Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the United States Department of Justice or the International Association of Chiefs of Police.

Every effort has been made by the IACP National Law Enforcement Policy Center staff and advisory board to ensure that this model policy incorporates the most current information and contemporary professional judgment on this issue. However, law enforcement administrators should be cautioned that no "model" policy can meet all the needs of any given law enforcement agency. Each law enforcement agency operates in a unique environment of federal court rulings, state laws, local ordinances, regulations, judicial and administrative decisions, and collective bargaining agreements that must be considered. In addition, the formulation of specific agency policies must take into account local political and community perspectives and customs, prerogatives and demands; often divergent law enforcement strategies and philosophies; and the impact of varied agency resource capabilities, among other factors.

Appendix D

LEIU *Criminal Intelligence File Guidelines*

An International Intelligence Network

CRIMINAL INTELLIGENCE FILE GUIDELINES

Prepared by LEIU

Revised March 2002

LAW ENFORCEMENT INTELLIGENCE UNIT

FOREWORD

These guidelines are provided to member agencies as an ongoing effort by your Executive Board to promote professionalism, provide protection for citizens' privacy, and yet enable law enforcement agencies to collect information in their pursuit of organized crime entities. It has long been established that agencies engaged in the collection, storage, analysis, and dissemination of criminal intelligence information must operate under specified guidelines to ensure abuses to this process do not occur. Along with operational guidelines, it is essential that member agencies adopt file procedures as a check and balance against inappropriate activities.

Each member agency is encouraged to have a written policy regarding its file procedures. A member may wish to adopt these guidelines or modify them to meet its particular state or local policies, laws, or ordinances. Member agencies with existing written file policies are commended and are encouraged to examine this document for any ideas that may augment their guidelines.

L.E.I.U. and its member agencies are in the forefront in promoting the value of the criminal intelligence function as a tool on combating organized crime and terrorism. Please do not hesitate to contact members of your Executive Board if you have questions, wish to discuss new ideas, or have suggestions for training.

Sincerely,

Richard Wright
General Chairman
Law Enforcement Intelligence Unit

CRIMINAL INTELLIGENCE FILE GUIDELINES

I. CRIMINAL INTELLIGENCE FILE GUIDELINES

These guidelines were established to provide the law enforcement agency with an information base that meets the needs of the agency in carrying out its efforts to protect the public and suppress criminal operations. These standards are designed to bring about an equitable balance between the civil rights and liberties of citizens and the needs of law enforcement to collect and disseminate criminal intelligence on the conduct of persons and groups who may be engaged in systematic criminal activity.

II. CRIMINAL INTELLIGENCE FILE DEFINED

A criminal intelligence file consists of stored information on the activities and associations of:

A. Individuals who:

1. Are suspected of being involved in the actual or attempted planning, organizing, financing, or commission of criminal acts; or

2. Are suspected of being involved in criminal activities with known or suspected crime figures.

B. Organizations, businesses, and groups that:

1. Are suspected of being involved in the actual or attempted planning, organizing, financing, or commission of criminal acts; or

2. Are suspected of being operated, controlled, financed, or infiltrated by known or suspected crime figures for use in an illegal manner.

III. FILE CONTENT

Only information with a criminal predicate and which meets the agency's criteria for file input should be stored in the criminal intelligence file. Specifically <u>excluded</u> material includes:

A. Information on an individual or group merely on the basis that such individual or group supports unpopular causes.

B. Information on an individual or group merely on the basis of ethnic background.

C. Information on any individual or group merely on the basis of religious or political affiliations.

D. Information on an individual or group merely on the basis of non-criminal personal habits.

E. Criminal Offender Record Information (CORI), should be excluded from an intelligence file. This is because CORI may be subject to specific audit and dissemination restrictions which are designed to protect an individual's right to privacy and to ensure accuracy.

F. Also excluded are associations with individuals that are not of a criminal nature.

State law or local regulations may dictate whether or not public record and intelligence information should be kept in separate files or commingled. Some agencies believe that separating their files will prevent the release of intelligence information in the event a subpoena is issued. This belief is unfounded, as all information requested in the subpoena (both public and intelligence) must be turned over to the court. The judge then makes the determination on what information will be released.

The decision to commingle or separate public and intelligence documents is strictly a management decision. In determining this policy, administrators should consider the following:

A. Records relating to the conduct of the public's business that are prepared by a state or local agency, regardless of physical form or characteristics, may be considered public and the public has access to these records.

B. Specific types of records (including intelligence information) may be exempt from public disclosure.

C. Regardless of whether public record information is separated from or commingled with intelligence data, the public may have access to public records.

D. The separation of public information from criminal intelligence information may better protect the confidentiality of the criminal file. If a request is made for public records, an agency can release the public file and leave the intelligence file intact (thus less apt to accidentally disclose intelligence information).

E. Separating of files is the best theoretical approach to maintaining files; however, it is not easy to do. Most intelligence reports either reference public record information or else contain a combination of intelligence and public record data. Thus, it is difficult to isolate them from each other. Maintaining separate public and intelligence files also increases the amount of effort required to index, store, and retrieve information.

IV. FILE CRITERIA

All information retained in the criminal intelligence file should meet file criteria prescribed by the agency. These criteria should outline the agency's crime categories and provide specifics for determining whether subjects involved in these crimes are suitable for file inclusion.

File input criteria will vary among agencies because of differences in size, functions, resources, geographical location, crime problems, etc. The categories listed in the suggested model below are not exhaustive.

A. Permanent Status

1. Information that relates an individual, organization, business, or group is suspected of being involved in the actual or attempted planning, organizing, financing, or committing of one or more of the following criminal acts:

    - Narcotic trafficking/manufacturing
    - Unlawful gambling
    - Loansharking
    - Extortion
    - Vice and pornography
    - Infiltration of legitimate business for illegitimate purposes
    - Stolen securities
    - Bribery
    - Major crime including homicide, sexual assault, burglary, auto theft, kidnapping, destruction of property, robbery, fraud, fencing stolen property, and arson
    - Manufacture, use, or possession of explosive devices for purposes of fraud, intimidation, or political motivation
    - Threats to public officials and private citizens.

2. In addition to falling within the confines of one or more of the above criminal activities, the subject/entity to be given permanent status must be identifiable--distinguished by a name and unique identifying characteristics (e.g., date of birth, criminal identification number, driver's license number, address). Identification at the time of file input is necessary to distinguish the subject/entity from existing file entries and those that may be entered at a later time. NOTE: The exception to this rule involves modus operandi (MO) files. MO files describe a unique method of operation for a specific type of crime (homicide, fraud) and may not be immediately linked to an identifiable suspect. MO files may be retained indefinitely while additional identifiers are sought.

B. Temporary Status:

Information that does not meet the criteria for permanent storage but may be pertinent to an investigation involving one of the categories previously listed should be given "temporary" status. It is recommended the retention of temporary information not exceed one year unless a compelling reason exists to extend this time period. (An example of a compelling reason is if several pieces of information indicate that a crime has been committed, but more than a year is needed to identify a suspect.) During this period, efforts should be made to identify the subject/entity or validate the information so that its final status may be determined. If the information is still classified temporary at the end of the one-year period, and a compelling reason for its retention is not evident, the information should be purged. An individual, organization, business, or group may be given temporary status in the following cases:

1. **Subject/entity is unidentifiable** - subject/entity (although suspected of being engaged in criminal activities) has no known physical descriptors, identification numbers, or distinguishing characteristics available.

2. **Involvement is questionable** - involvement in criminal activities is suspected by a subject/entity which has either:

    - **Possible criminal associations** - individual, organization, business, or group (not currently reported to be criminally active) associates with a known criminal and appears to be jointly involved in illegal activities.

    - **Criminal history** - individual, organization, business, or group (not currently reported to be criminally active) that has a history of criminal conduct, and the circumstances currently being reported (i.e., new position or ownership in a business) indicates they may again become criminally active.

3. **Reliability/validity unknown** - the reliability of the information sources and/or the validity of the information cannot be determined at the time of receipt; however, the information appears to be significant and merits temporary storage while verification attempts are made.

V. INFORMATION EVALUATION

Information to be retained in the criminal intelligence file should be evaluated and designated for reliability and content validity prior to filing.

The bulk of the data an intelligence unit receives consists of unverified allegations or information. Evaluating the information's source and content indicates to future users the information's worth and usefulness. Circulating information which may not have been evaluated, where the source reliability is poor or the content validity is doubtful, is detrimental to the agency's operations and contrary to the individual's right to privacy.

To ensure uniformity with the intelligence community, it is strongly recommended that stored information be evaluated according to the criteria set forth below.

Source Reliability:

(A) **Reliable** - The reliability of the source is unquestioned or has been well tested in the past.

(B) **Usually Reliable** - The reliability of the source can usually be relied upon as factual. The majority of information provided in the past has proven to be reliable.

(C) **Unreliable** - The reliability of the source has been sporadic in the past.

(D) **Unknown** -The reliability of the source cannot be judged. Its authenticity or trustworthiness has not yet been determined by either experience or investigation.

Content Validity:

(1) **Confirmed** - The information has been corroborated by an investigator or another independent, reliable source.

(2) **Probable** - The information is consistent with past accounts.

(3) **Doubtful** - The information is inconsistent with past accounts.

(4) **Cannot Be Judged** - The information cannot be judged. Its authenticity has not yet been determined by either experience or investigation.

VI. INFORMATION CLASSIFICATION

Information retained in the criminal intelligence file should be classified in order to protect sources, investigations, and the individual's right to privacy. Classification also indicates the internal approval which must be completed prior to the release of the information to persons outside the agency. However, the classification of information in itself is not a defense against a subpoena duces tecum.

The classification of criminal intelligence information is subject to continual change. The passage of time, the conclusion of investigations, and other factors may affect the security classification assigned to particular documents. Documents within the intelligence files should be reviewed on an ongoing basis to ascertain whether a higher or lesser degree of document security is required to ensure that information is released only when and if appropriate.

Classification systems may differ among agencies as to the number of levels of security and release authority. In establishing a classification system, agencies should define the types of information for each security level, dissemination criteria, and release authority. The system listed below classifies data maintained in the Criminal Intelligence File according to one of the following categories:

Sensitive

1. Information pertaining to significant law enforcement cases currently under investigation.
2. Corruption (police or other government officials), or other sensitive information.
3. Informant identification information.
4. Criminal intelligence reports which require strict dissemination and release criteria.

Confidential

1. Criminal intelligence reports not designated as sensitive.
2. Information obtained through intelligence unit channels that is not classified as sensitive and is for law enforcement use only.

Restricted

1. Reports that at an earlier date were classified sensitive or confidential and the need for high-level security no longer exists.
2. Non-confidential information prepared for/by law enforcement agencies.

Unclassified

1. Civic-related information to which, in its original form, the general public had direct access (i.e., public record data).
2. News media information - newspaper, magazine, and periodical clippings dealing with specified criminal categories.

VII. INFORMATION SOURCE

In all cases, source identification should be available in some form. The true identify of the source should be used unless there is a need to protect the source. Accordingly, each law enforcement agency should establish criteria that would indicate when source identification would be appropriate.

The value of information stored in a criminal intelligence file is often directly related to the source of such information. Some factors to consider in determining whether source identification is warranted include:

- The nature of the information reported.
- The potential need to refer to the source's identity for further or prosecutorial activity.
- The reliability of the source.

Whether or not confidential source identification is warranted, reports should reflect the name of the agency and the reporting individual. In those cases when identifying the source by name is not practical for internal security reasons, a code number may be used. A confidential listing of coded sources of information can then be retained by the intelligence unit commander. In addition to identifying the source, it may be appropriate in a particular case to describe how the source obtained the information (for example "S-60, a reliable police informant heard" or "a reliable law enforcement source of the police department saw" a particular event at a particular time).

VIII. INFORMATION QUALITY CONTROL

Information to be stored in the criminal intelligence file should undergo a thorough review for compliance with established file input guidelines and agency policy prior to being filed. The quality control reviewer is responsible for seeing that all information entered into the criminal intelligence files conforms with the agency's file criteria and has been properly evaluated and classified.

IX. FILE DISSEMINATION

Agencies should adopt sound procedures for disseminating stored information. These procedures will protect the individual's right to privacy as well as maintain the confidentiality of the sources and the file itself.

Information from a criminal intelligence report can only be released to an individual who has demonstrated both a "need-to-know" and a "right-to-know."

"Right-to-know" Requestor has official capacity and statutory authority to the information being sought.

"Need-to-know" Requested information is pertinent and necessary to the requestor agency in initiating, furthering, or completing an investigation.

No "original document" which has been obtained from an outside agency is to be released to a third agency. Should such a request be received, the requesting agency will be referred to the submitting agency for further assistance.

Information classification and evaluation are, in part, dissemination controls. They denote who may receive the information as well as the internal approval level(s) required for release of the information. In order to encourage conformity within the intelligence community, it is recommended that stored information be classified according to a system similar to the following.

Security Level	Dissemination Criteria	Release Authority
Sensitive	Restricted to law enforcement personnel having a specific need-to-know and right-to-know	Intelligence Unit Commander
Confidential	Same as for sensitive	Intelligence Unit Manager or designee
Restricted	Same as for Sensitive	Intelligence Unit Supervisor or designee
Unclassified	Not restricted	Intelligence Unit Personnel

The integrity of the criminal intelligence file can be maintained only by strict adherence to proper dissemination guidelines. To eliminate unauthorized use and abuses of the system, a department should utilize a dissemination control form that could be maintained with each stored document. This control form would record the date of the request, the name of the agency and individual requesting the information, the need-to-know, the information provided, and the name of the employee handling the request. Depending upon the needs of the agency, the control form also may be designed to record other items useful to the agency in the management of its operations. This control form also may be subject to discovery.

X. FILE REVIEW AND PURGE

Information stored in the criminal intelligence file should be reviewed periodically for reclassification or purge in order to: ensure that the file is current, accurate, and relevant to the needs and objective of the agency; safeguard the individual's right of privacy as guaranteed under federal and state laws; and, ensure that the security classification level remains appropriate.

Law enforcement agencies have an obligation to keep stored information on subjects current and accurate. Reviewing of criminal intelligence should be done on a continual basis as agency personnel use the material in carrying out day-to-day activities. In this manner, information that is no longer useful or that cannot be validated can immediately be purged or reclassified where necessary.

To ensure that all files are reviewed and purged systematically, agencies should develop purge criteria and schedules. Operational procedures for the purge and the method of destruction for purged materials should be established.

A. Purge Criteria:

General considerations for reviewing and purging of information stored in the criminal intelligence file are as follows:

1. Utility

How often is the information used?
For what purpose is the information being used?
Who uses the information?

2. Timeliness and Appropriateness

Is this investigation still ongoing?
Is the information outdated?
Is the information relevant to the needs and objectives of the agency?
Is the information relevant to the purpose for which it was collected and stored?

3. Accuracy and Completeness

Is the information still valid?
Is the information adequate for identification purposes?
Can the validity of the data be determined through investigative techniques?

B. Review and Purge Time Schedule:

Reclassifying and purging information in the intelligence file should be done on an ongoing basis as documents are reviewed. In addition, a complete review of the criminal intelligence file for purging purposes should be undertaken periodically. This review and purge schedule can vary from once each year for documents with temporary status to once every five years for permanent documents. Agencies should develop a schedule best suited to their needs and should contact their legal counsel for guidance.

C. Manner of Destruction:

Material purged from the criminal intelligence file should be destroyed. Disposal is used for all records or papers that identify a person by name. It is the responsibility of each agency to determine that their obsolete records are destroyed in accordance with applicable laws, rules, and state or local policy.

XI. FILE SECURITY

The criminal intelligence file should be located in a secured area with file access restricted to authorized personnel.

Physical security of the criminal intelligence file is imperative to maintain the confidentiality of the information stored in the file and to ensure the protection of the individual's right to privacy.

Glossary

PUBLIC RECORD

Public record includes any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics.

"Member of the public" means any person, except a member, agent, officer, or employee of a federal, state, or local agency acting within the scop of his or her membership in an agency, office, or employment.

For purposes of these guidelines, public record information includes only that information to which the general public normally has direct access, (i.e., birth or death certificates, county recorder's information, incorporation information, etc.)

CRIMINAL OFFENDER RECORD INFORMATION (CORI)

CORI is defined as summary information to arrests, pretrial proceedings, sentencing information, incarcerations, parole and probation.

a. Summary criminal history records are commonly referred to as "rap sheets." Data submitted on fingerprint cards, disposition of arrest and citation forms and probation flash notices create the entries on the rap sheet.

Appendix E

Criminal Intelligence Training Standards For United States Law Enforcement and Other Criminal Justice Agencies

Draft
Policy Recommendation

Criminal Intelligence Training Standards for United States Law Enforcement and Other Criminal Justice Agencies

By

The Global Justice Information Sharing Initiative
Intelligence Working Group (GIWG)
Training Committee

April 13, 2003

Criminal Intelligence Training Standards for United States Law Enforcement and Other Criminal Justice Agencies

Background

The International Association of Chiefs of Police (IACP) and the Community Oriented Policing Services (COPS) "Summit on Criminal Information Sharing: Overcoming Barriers to Enhance Domestic Security" underscored the need to establish standards for intelligence training.

The IACP *Criminal Intelligence Sharing Report: A National Plan for Intelligence-Led Policing at the Local, State and Federal Level*, included the recommendation to: "promote intelligence-led policing through a common understanding of criminal intelligence and its usefulness."

The IACP "Core Recommendations to Achieving the Plan" identified several intelligence-training issues:

- Training should provide recipients with the skills to provide targeted, evaluative summary data to decision makers.
- Appropriate training must be provided to both current and entering law enforcement personnel on information sharing systems and criminal intelligence concepts.
- Training should promote building trust for intelligence sharing and maintaining civil rights/constitutional protections.
- Training should emphasize that all personnel, regardless of their job, have a role in intelligence and sharing information.
- Training should equip personnel to use new technologies.

Standards for training on intelligence functions are critical to implementing a national model for intelligence-led policing. National intelligence training standards can provide criminal justice agencies, individually and collectively, with the framework for achieving that end.

The goal of the training is to professionalize and enhance the practice of criminal intelligence within the United States law enforcement/criminal justice community, demonstrate the benefits derived from the intelligence, and encourage information sharing in support of the intelligence.

Purpose of Standards

The purpose of these standards is to establish core concepts, principles, and practices within the law enforcement criminal intelligence function. This, in turn, will promote the sharing_of information and increase cooperation among law enforcement to better protect the public from criminal enterprises and threats.

Scope

The Global Justice Information Sharing Initiative (Global) Intelligence Working Group (GIWG) Training Committee adopted the IACP Summit participants' training recommendations that all levels of law enforcement need to be trained in intelligence. Otherwise, intelligence could become solely the focus of a small unit within the department, rather than being part of the core mission in which all levels of the department are involved.

The GIWG Training Committee focused on a train-the-trainer component and establishing standards for police executives, managers of criminal intelligence/investigative functions, general law enforcement officers, intelligence officers, and intelligence analysts. The Committee's first goal is to identify specific training topics and issues for each level of personnel involved in the intelligence process. Their second goal is to make specific recommendations for training objectives and the delivery of training. Their third goal is to work with relevant agencies and groups to develop model curricula.

The GIWG Training Committee discussed and reviewed key law enforcement criminal intelligence organizations' methods and best practices. The intelligence training standards developed by the committee were based upon core concepts, subjects, and essential functions of the law enforcement criminal intelligence process.

Approximately 19 intelligence training curricula, representing international, national, state and local level programs, were reviewed. The programs contained a variety of subjects and approaches to instructing/learning methods. The number of programs narrowed drastically when looking for differing programs, not commercially-based, and associated with reputable and knowledgeable organizations. During the research phase the Committee noted the lack of national level training standards and absence of any single national agency coordinating intelligence training.

Local, state, and federal governmental agencies as well as private/non-profit professional associations provide intelligence training. There is no one source or set of comprehensive curricula that meets the goals of the GIWG Training Committee. Their effort, then, was to draw from the varied sources of training, identify training that needed to be developed, and put it together in a cohesive training package.

Global Intelligence Working Group (GIWG)

Intelligence Training Standards Policy Statement

Law enforcement and other criminal justice agencies engaged in the planning, collection, collation, analysis, and dissemination of information and criminal intelligence shall meet criminal intelligence training standards to ensure professional conduct and the capability to achieve a common understanding of intelligence-led policing. Complying with the intelligence training standards requires:

- Training all levels of personnel involved in the sharing of information and intelligence management and operational process.
- Promoting the understanding and learning of core principles, concepts and practices in intelligence-led policing operations and the management of the intelligence function.
- Making intelligence training mandatory for those involved in the national criminal intelligence sharing system.

These standards shall be considered national intelligence training standards, created to serve as a blueprint for developing core knowledge necessary to achieve an intelligence-led policing capability within every law enforcement agency. The intelligence training policy standards represent the minimum training objectives for agencies performing intelligence functions.

It is important to note that this committee recognizes the difficulties associated with the implementation and subsequent delivery of a new suggested training for state and local law enforcement officers.

It is imperative that all Peace Officer Standards and Training Committees (POST) of this nation be contacted and become partners in the training proposals. The POST commissions should act as liaisons to ensure intelligence training is mandated and delivered to all law enforcement personnel.

Once implemented, the criminal intelligence curriculum should be evaluated in order to determine its effectiveness.

Global Intelligence Working Group (GIWG)

Intelligence Training Standards

Law Enforcement Officers *(Level One)*

Role

The role of law enforcement officers, relative to intelligence, is to be cognizant they play a crucial part in reducing crime by collecting information that may reflect or indicate criminal activity. Law enforcement officers are the largest and most viable information collection resource available within the law enforcement community.

Mission

The intelligence mission of each law enforcement officer is to support the agency's criminal intelligence function by collecting and reporting indications of criminal activity and suspicious individuals.

Core Training Objectives

I. Law enforcement officers will understand the criminal intelligence process and its ability to enhance their contributions to the criminal justice system.

II. Law enforcement officers will be provided with information on available data systems, networks, and resources.

III. Law enforcement officers will be able to identify key signs of criminal activity and procedures for collecting data on and reporting such activity.

IV. Law enforcement officers will gain an understanding of the legal, privacy, and ethical limitations placed on the collection of criminal intelligence information.

Training Length and Delivery

The two-hour training for law enforcement officers should be presented in an academy classroom environment (basic training or in-service), during roll calls, or through video teleconference (e.g., California and Arizona Peace Officer Standards Training Board) format. Training materials should be developed and provided to state level training standards boards for inclusion into basic training curricula.

Global Intelligence Working Group (GIWG)

Intelligence Training Standards
Law Enforcement Executives *(Level Two)*

Role

The role of the chief executive is to ensure the intelligence function is management-directed and complies with every law and regulation governing collection, storage, and dissemination/use of criminal information and intelligence. The executive shall also establish an intelligence-led policing environment that promotes the sharing of information and development of criminal intelligence.

Mission

The intelligence mission of the chief executive is to ensure the administration, monitoring, and control of the organization's criminal intelligence function is effective and ethical. Establishing the proper environment allows the intelligence process to produce timely, relevant, and actionable criminal intelligence that supports the mission of the organization.

Core Training Objectives

I. Executives will understand the criminal intelligence process and the role the process plays in enhancing public safety.

II. Executives will understand the philosophy of intelligence-led policing and their own role in the National Criminal Intelligence Sharing Plan.

III. Executives will understand the legal, privacy, and ethical issues relating to criminal intelligence.

IV. Executives will be provided with information on existing criminal information sharing networks and resources available in support of their agencies.

Training Length and Delivery

Training is four hours and should be delivered in a classroom style or conference environment whenever possible. Training should be delivered by other law enforcement executives or executives in combination with intelligence professionals.

Global Intelligence Working Group (GIWG)

Intelligence Training Standards
Intelligence Commanders/Supervisors *(Level Three)*

Role

The role of the intelligence commander/supervisor is to ensure the daily intelligence function operates in accord with the agency's policies and intelligence collection requirements. The commander/supervisor role also involves managing the accountability for the functioning of the intelligence process; ensuring the intelligence structure of the organization is organized and staffed with properly trained and skilled personnel; and ensuring there are adequate resources for producing intelligence/knowledge products.

Mission

The mission of the intelligence commander/supervisor is to manage and direct the agency's criminal intelligence programs. Through establishing the proper environment, the commander/supervisor may ensure that the intelligence function produces timely, relevant, and actionable criminal intelligence that supports the mission of the organization.

Core Training Objectives

I. Managers will understand the criminal intelligence process, intelligence-led policing, and their roles in enhancing public safety.

II. Managers will be provided with information on training, evaluating and assessing an effective criminal intelligence function.

III. Managers will understand the unique issues of a criminal intelligence unit, including personnel selection, ethics, developing policies and procedures, and promoting intelligence products.

IV. Managers will understand the principles and practices of handling sensitive information, informant policies, and corruption prevention and recognition.

V. Managers will understand the legal and privacy issues surrounding the criminal intelligence environment.

VI. Managers will understand the processes necessary to produce tactical and strategic intelligence products.

VII. Managers will be provided with information on criminal information sharing systems, networks, and resources available to their agencies.

VIII. Managers will understand the development process and implementation of collection plans.

Training Length and Delivery

The intelligence commanders/supervisors training is 24 hours and should be delivered in a classroom environment. Regional or statewide training of intelligence commanders would probably be the best approach. A detailed curriculum for this level of training should be developed by the GIWG Training Committee, in conjunction with established intelligence programs and associations, and provided to state agencies with intelligence training responsibilities. (See the train-the-trainer component.)

Global Intelligence Working Group (GIWG)

Intelligence Training Standards
Intelligence Officers/Collectors *(Level Four)*

Role

The intelligence officer's role is to collect, evaluate, and compile information in support of specific agency collection requirements or operations. The role of intelligence officers frequently extends beyond their agencies and requires them to create external information networks and to support other agencies' information and intelligence requests.

The intelligence officer's role also involves evaluating both source and information, preparing written reports and assessments, giving briefings, determining the need-to-know/right-to-know about specific activities, and protecting citizens' rights to privacy.

Mission

The mission of the intelligence officer is to support the agency's criminal intelligence requirements/assessments though the collection and handling of information, using proper investigative and intelligence gathering practices.

Core Training Objectives

I. Intelligence officers will understand the criminal intelligence process and their critical role in the process.

II. Intelligence officers will understand the legal, ethical, and privacy issues surrounding criminal intelligence and their liability as intelligence information collectors.

III. Intelligence officers will be provided with information on Internet resources, information sharing systems, networks, and other sources of information.

IV. Intelligence officers will gain an understanding of the proper handling of criminal intelligence information, including file management and information evaluation.

V. Intelligence officers will understand the processes of developing tactical and strategic products and experience the development of some products.

VI. Intelligence officers will experience the development of criminal intelligence from information through the critical thinking/inference development process.

VII. Intelligence officers will understand the tasks of building and implementing collection plans.

Training Length and Delivery

The intelligence officer/collector training is 40 hours long and should be delivered in a classroom environment. Delivery at the statewide or regional level by local, state, and federal police training agencies, intelligence professional associations, and/or qualified private law enforcement training companies would probably be the best approach. A detailed curriculum for this level of training should be developed by the GIWG Training Committee, in conjunction with established intelligence programs and associations, and provided to state agencies with intelligence training responsibilities. (See the train-the-trainer component.)

Global Intelligence Working Group (GIWG)

Intelligence Training Standards
Intelligence Analysts *(Level Five)*

Role

The intelligence analyst's role is to collect, evaluate, analyze, and disseminate information in support of specific agency collection requirements or operations. Before information can become intelligence, it must be analyzed. Therefore the intelligence analyst's role is vital to the production of usable, timely, and comprehensive intelligence. Intelligence analysts systematically organize, research, compare, and analyze information. They produce assessments of criminal activity, tactical and strategic intelligence collection plans, and documents that allow management to maximize the agency's resources.

Mission

The mission of the intelligence analyst is to research and analyze raw data, apply critical thinking and logic skills to develop sound conclusions and recommendations, and provide actionable intelligence in a cohesive and clear manner to management.

Core Training Objectives

I. Intelligence analysts will understand the criminal intelligence process, intelligence-led policing, and their roles in enhancing public safety.

II. Analysts will understand the importance of the National Criminal Intelligence Sharing Plan and the role it plays in reducing crime and violence throughout the country.

III. Analysts will gain an understanding of the proper handling of criminal intelligence information, including file management and information evaluation.

IV. Analysts will experience the development of intelligence through the processes of critical thinking, logic, inference development, and recommendation development.

V. Analysts will understand the tasks of building and implementing collection and analytic plans.

VI. Analysts will be familiar with the legal, privacy, and ethical issues relating to intelligence.

VII. Analysts will be provided with information on research methods and sources including the Internet, information sharing systems, networks, centers, commercial and public databases, and other sources of information.

VIII. Analysts will demonstrate a practical knowledge of the methods and techniques employed in analysis including, but not limited to: crime pattern analysis, association analysis, telephone record analysis, flow analysis, spatial analysis, financial analysis, and strategic analysis.

IX. Analysts will be familiar with the skills underlying analytic methods including report writing, statistics, and graphic techniques.

X. Analysts will be familiar with available computer programs that support the intelligence function including database, data/text mining, visualization, and mapping software.

Training Length and Delivery

The intelligence analyst training is a minimum of 40 hours and should be delivered in a classroom environment. The training should be provided by individuals with analytic experience in local, state, or federal police training agencies (that may be training on behalf of those agencies), intelligence professional associations, or qualified private law enforcement training companies.

This is the area of intelligence in which the most training is currently available. Structured courses have been given for three decades, and new or revised models are constantly arising.

Global Intelligence Working Group (GIWG)

Intelligence Training Standards
Train-the-Trainer *(Level Six)*

Role

It is necessary to train people to deliver the different levels of courses before they can be provided, particularly for Levels 3 and 4. (Levels 1 and 2 are a half day or less and program materials can be easily developed and provided to potential training organizations.)

Mission

The mission of the trainer is to provide an overview of materials developed for presentation to Intelligence Commanders/Supervisors and Intelligence Officers to support the nationwide intelligence training initiative and to be fully capable of providing the assigned training.

Core Training Objectives

I. Trainers will understand the intelligence process and how it functions.

II. Trainers will understand the importance of the National Criminal Intelligence Sharing Plan and the role it plays in reducing crime and violence throughout the country.

III. Trainers will be provided with information on a variety of sources of information and how these may be researched and updated.

IV. Trainers will understand the processes of developing tactical and strategic products.

V. Trainers will understand the methods and techniques of adult learning.

VI. Trainers will be familiar with the use of audiovisual aids available.

VII. Trainers will be provided with all course materials and guidance on all course exercises.

VIII. Trainers will be aware of the legal, privacy, and ethical issues relating to intelligence.

IX. Trainers will prepare and present a short module on intelligence.

Training Length and Delivery

Train-the-trainer training is 40 plus hours and should be delivered in a classroom environment. However, those being trained should be provided with all Commander/Supervisor and Intelligence Officer training materials in advance so they may become familiar with them. They should also be provided with copies of source material being used in the class (e.g., laws, policies, standards, *Intelligence 2000: Revising the Basic Elements*, etc.) and should be committed to reviewing all of these before attending the class. This would require approximately 25 hours of reading and study.

The train-the-trainer class should be provided by agencies with established intelligence programs and intelligence professional associations, in conjunction with the GIWG Training Committee.

Resources to Support Training

To develop and provide the training noted in these standards, further work must be done to develop specific curricula, training aids, and exercises.

Some training models or modules are already found in Internet-based and interactive CD-ROMs such as the International Association of Law Enforcement Intelligence Analysts (IALEIA), National White Collar Crime Center and Law Enforcement Intelligence Unit (LEIU) "Turn Key Intelligence"; U.S. Army Military School's - Analytical Investigative Tools; the Joint Military Intelligence Training Center, DIA, Counter-Drug Intelligence Analysis course; the National High Intensity Drug Trafficking Area Assistance Center, "Analysis and Critical Thinking"; as well as California and Arizona POST Board curricula.

Literature such as the IALEIA and LEIU *Intelligence 2000: Revising the Basics Elements* can be used to study foundations of the criminal intelligence process, while other books and booklets published by the two groups (including a booklet on *Intelligence-Led Policing* distributed by IALEIA) can also be of assistance.

There are models for all levels of training recommended in these standards. The GIWG Training Committee will work further to provide a distillation of those models and modules into a comprehensive set of curricula for the benefit of law enforcement nationwide.

Appendix F

GIWG Outreach Plan

Outreach Plan

Those items denoted with an asterisk have already been completed.

- *Develop marketing materials that provide a historical perspective on the National Criminal Intelligence Sharing Plan and explain the GIWG mission and goals
  - Four-page handout
  - Eight-page information brochure
  - News article
  - PowerPoint presentations
  - Quotes from key practitioners regarding the value of the National Criminal Intelligence Sharing Plan

- *Identify media to utilize for distribution of the marketing materials
  - Criminal justice publications (e.g., IACP Police Chief, FBI Bulletin, IALEIA Journal, etc.
  - Web sites (www.it.ojp.gov) (www.iir.com)
  - Newspapers

- *Identify target audiences for marketing the Plan
  - National conferences/annual meetings of law enforcement organizations (e.g., IACP, LEIU, National Sheriffs' Association)
  - Local and state law enforcement associations/organizations
  - Task forces
  - Local agency roll calls
  - Training academies
  - Private training providers

- Develop a "package" to utilize when conducting outreach efforts
  - Letter template
  - Brochures
  - CD with PowerPoint presentation
  - News article for publication
  - Privacy information

- Utilize partner organizations that focus on information sharing to endorse and promote the Plan (e.g., IACP, National Sheriffs' Association, Prosecutors, LEIU, IALEIA, IADLEST) by requesting passage of resolutions promoting the National Criminal Intelligence Sharing Plan

- Develop a logo that represents the Plan and distribute to participating agencies and partner organizations/associations for posting on their Web sites along with a hyperlink to the National Criminal Intelligence Sharing Plan Web site

- Develop a poster and booklet containing key elements of the Plan, and make available for distribution after report is finalized

- Schedule one-on-one meetings with key contacts to obtain their consensus, endorsement, and participation in the Plan

  - Federal leadership and agencies
  - Governing entities of intelligence-sharing systems

- Develop a Web site accessible to appropriate law enforcement personnel (www.it.ojp.gov/global)

- *Develop a Train-the-Trainer application to increase the number of presenters available to make marketing/outreach presentations

- Request the Commission on Accreditation for Law Enforcement Agencies (CALEA) and state accrediting organizations modify their standards to incorporate the National Criminal Intelligence Sharing Plan's model standards

- Coordinate a mass distribution of the finalized National Criminal Intelligence Sharing Plan

- Develop marketing materials specifically geared towards public safety, correctional staff, and critical infrastructure communities

Appendix G

Developing a National Criminal Intelligence Plan
Article and Brochure

Global Intelligence Working Group

BJA

DEVELOPING A NATIONAL CRIMINAL INTELLIGENCE SHARING PLAN

Have they finally caught him?

Imagine a detective working a fraud investigation. As a result of a ***single*** inquiry into a networked system—connected to local, state, regional, and federal databases—responses are received from the Federal Bureau of Investigation and a state law enforcement agency that the subject is also a target of a major money laundering operation, which may be supplying several terrorist organizations. The detective then contacts the intelligence analyst listed as the point of contact in the networked system, who provides a comprehensive briefing document that explains how the detective's fraud investigation fits into the "big picture."

Save time! Save money! Create better intelligence systems!

Picture law enforcement executives preparing to develop an intelligence system. Instead of wading through a series of false starts, the executives have—at their fingertips—a source of established standards for managing intelligence data and ensuring system security. They will have access to established, proven model policies and standards that promote intelligence sharing, while ensuring individuals' rights to privacy.

Quality training for all.

Your staff could access quality intelligence training programs for all levels of personnel, regardless of the size or location of your law enforcement agency.

Is it too good to be true to have a single initiative addressing all these concerns? Not when the National Criminal Intelligence Sharing Plan is finalized and accepted.

What is the National Criminal Intelligence Sharing Plan?

The National Criminal Intelligence Sharing Plan ("Plan") is a formal intelligence sharing initiative that will securely link local, state, tribal, and federal law enforcement agencies, facilitating the exchange of critical intelligence information. The Plan contains model policies and standards and describes a nationwide communications capability that will link all levels of law enforcement personnel, including officers on the street, intelligence analysts, unit commanders, and police executives.

Why do we need it and how did it get started?

The need for a National Criminal Intelligence Sharing Plan arose out of the tragic events of September 11, 2001, when over 3,000 innocent lives were lost as a result of terrorist attacks against the United States.

When President George W. Bush called for the creation of a Cabinet-level agency to coordinate homeland security, he emphasized improved criminal intelligence sharing as ***critical*** to enhancing law enforcement and other emergency agencies' abilities to protect the American public.

May 2003

In fall 2001, law enforcement officers attending the International Association of Chiefs of Police (IACP) conference in Toronto, Canada, identified a need for an assessment to identify the inadequacies of the intelligence process that, in part, led to the failure to prevent the tragic events of September 11. As a result, law enforcement executives and intelligence experts joined resources at the IACP Criminal Intelligence Sharing Summit held in Alexandria, Virginia, in March 2002, and articulated a proposal for an intelligence sharing plan that was in alignment with the President's initiative. They envisioned non-federal, law enforcement agencies fully participating with federal agencies to coordinate, collect, analyze, and appropriately disseminate criminal intelligence data across the United States, to make our nation safer.

How is this collaboration achieved? Summit participants called for the creation of some type of criminal intelligence coordinating council. As planned, this collective, comprised of all types of law enforcement agencies, would develop and oversee the National Criminal Intelligence Sharing Plan. Key to the process was efficient leveraging of existing efforts—the commitment to ***build on***, not reinvent, substantial information sharing activities already underway. Joseph Polisar, Chief of Garden Grove, California, Police Department and IACP First Vice President, states, "The need for intelligence sharing is paramount to our nation's safety. It is absolutely critical that we break down the barriers and expeditiously implement a plan for intelligence sharing that is continuously emphasized and built upon." Summit recommendations also included:

- Development of standardized policies, operating procedures, and training guidelines
- Creation of an outreach strategy
- Protection of individuals' civil rights

Additional information on the IACP Summit can be located in *Recommendations from the IACP Intelligence Summit, Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing at the Local, State, and Federal Levels.*[1]

Who is developing it?

In fall 2002, in response to this crucial need, the U.S. Department of Justice, Office of Justice Programs (OJP), Bureau of Justice Assistance (BJA), authorized the formation of the Global Intelligence Working Group, one of several issue-focused subgroups of the Global Justice Information Sharing Initiative (Global) Advisory Committee.[2]

The Global Intelligence Working Group (GIWG) serves as the Criminal Intelligence Coordinating Council recommended by the IACP Summit participants. Comprehensive

[1] This document is available at: http://www.theiacp.org/documents/pdfs/Publications/intelsharingreport.pdf.

[2] Global, operating under the auspices of BJA, serves as an advisory body to the Federal Government—specifically through the Assistant Attorney General, OJP, and the U.S. Attorney General—in facilitating standards-based electronic information exchange throughout the justice and public safety communities. The Global Advisory Committee (GAC or "Committee") is comprised of key personnel from local, state, tribal, federal, and international justice and public safety entities, and includes agency executives and policymakers, automation planners and managers, information practitioners, and most importantly, end users. GAC membership reflects the fundamental Global tenet that the entire justice-interested community must be involved in information sharing. Global working groups, made up of Committee members and other subject-matter experts, expand the GAC's knowledge and experience. These groups are formed around timely issues impacting justice information sharing; the GIWG is one of four working groups. For more information on Global, please visit http://www.it.ojp.gov/global/.

law enforcement, and justice representation is achieved by participation from the following organizations and constituencies:

- Federal Bureau of Investigation
- High Intensity Drug Trafficking Areas
- International Association of Chiefs of Police
- International Association of Law Enforcement Intelligence Analysts
- INTERPOL-USNCB
- Justice Management Institute
- Law Enforcement Intelligence Unit
- Local, state, and tribal police agencies[3]
- Major Cities Chiefs Association
- National Conference of State Legislatures
- National Sheriffs' Association
- National White Collar Crime Center
- Prosecutors
- Regional Information Sharing Systems
- State Law Enforcement Intelligence Networks
- U.S. Drug Enforcement Administration
- U.S. Department of Homeland Security
- U.S. Department of Justice

What are the challenges?

Members of the GIWG realize that challenges lie before them. The GIWG is committed to overcoming longstanding, historical barriers hindering intelligence sharing, as well as future impediments that may develop. They acknowledge a major component will be informing all relevant communities of the existence of the National Criminal Intelligence Sharing Plan while recognizing that immediate acceptance of the Plan is not guaranteed. Ongoing training and education will be a major factor in the successful implementation and continuation of this National Criminal Intelligence Sharing Plan effort.

How will the National Criminal Intelligence Sharing Plan meet those challenges? What will it look like?

The GIWG mission is to develop, build, and support the creation of the National Criminal Intelligence Sharing Plan, which will provide justice-related agencies with the ability to gather, analyze, protect, and share information and intelligence to identify, investigate, prevent, deter, and defeat criminal and terrorist activities, both domestically and internationally, as well as protect the security of our homeland and preserve the rights and freedoms of all Americans.

Using the above mission as a foundation to build upon, the GIWG members articulated a *vision* of what the National Criminal Intelligence Sharing Plan should be to local, state, tribal, and federal law enforcement agencies:

- Model intelligence sharing plan
- Mechanism to provide seamless sharing of information between systems
- Model for intelligence process principles and policies
- National model for training on intelligence
- Outreach model to promote intelligence sharing
- Model for protecting individuals' privacy and civil rights

[3] Local, state, and tribal law enforcement representatives are key participants and stakeholders in the development of this Plan. It is believed that their familiarity with local processes will contribute towards the Plan's successful implementation.

- Blueprint for law enforcement administrators to follow when reviewing their own intelligence system or building a new one
- Mechanism to promote intelligence-led policing

To best address the IACP Summit recommendations and realize the above-listed tenets of the vision, the GIWG is divided into committees. The committees have identified goals and associated tasks, including identifying necessary policies and frameworks for implementing standards-based intelligence sharing; identifying standards for collection, collation, storage, analysis, evaluation, and dissemination of intelligence information; ensuring compatibility of policies, standards, guidelines, and operating procedures of current and proposed intelligence sharing systems; and ensuring protection of individuals' privacy and civil rights. They will also develop an outreach plan to publicize and aid in institutionalizing the National Criminal Intelligence Sharing Plan, and a training plan supporting a standards-based intelligence system for all levels of law enforcement. The GIWG understands that intelligence sharing cannot occur without trust between the parties sharing information. Thus, one of the central tasks of the GIWG is to increase communication, strengthen relationships, and help build trust between agencies and individuals in the intelligence network.

Mr. Melvin Carraway, Chairman of the GIWG and Superintendent of the Indiana State Police, related, "The Intelligence Working Group is focusing on overcoming the impediments to intelligence sharing." Chairman Carraway stressed the importance of the GIWG's work to public safety and homeland security by stating, "Making the benefits of the National Criminal Intelligence Sharing Plan clear to patrol officers, detectives, intelligence unit managers, law enforcement executives, and federal officers is key to the GIWG vision." Additionally, past IACP President Bill Berger, Chief of the North Miami Beach, Florida, Police Department, emphasized the value of a national intelligence sharing plan. He stated, "Imagine the ability to have access to a comprehensive document that would enable law enforcement officials to develop a new system utilizing established and proven policies and standards. The National Criminal Intelligence Sharing Plan will do that and more."

When will the National Criminal Intelligence Sharing Plan be available?

The GIWG will provide an interim report containing preliminary recommendations to BJA in May 2003. The final report is due in October 2003 and will be posted on the Global web site.

For More Information—

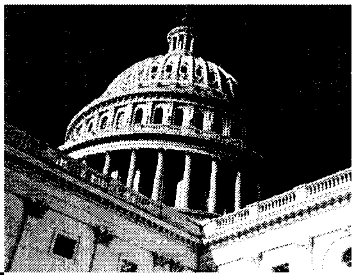
More information about the National Criminal Intelligence Sharing Plan or GIWG can be obtained from the Global web site www.it.ojp.gov/global. In addition, presentations and briefings regarding the National Criminal Intelligence Sharing Plan are anticipated at upcoming association and organizational meetings for groups such as the IACP, Law Enforcement Intelligence Unit, National Sheriffs' Association, Major Cities Chiefs Association, International Association of Law Enforcement Intelligence Analysts, and the National Organization of Black Law Enforcement Executives.

DEPARTMENT OF JUSTICE
QUI PRO DOMINA JUSTITIA SEQUITUR
OFFICE OF JUSTICE PROGRAMS

Global Intelligence Working Group:

Global Justice Information Sharing Initiative

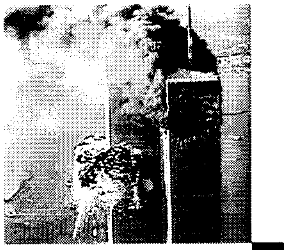
Developing a National Criminal Intelligence Sharing Plan

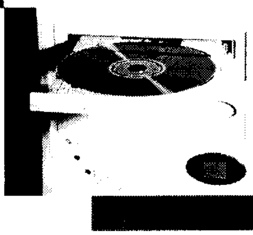


What is the National Criminal Intelligence Sharing Plan?

The need for a National Criminal Intelligence Sharing Plan arose out of the tragic events of September 11, 2001, when over 3,000 innocent lives were lost as a result of terrorist attacks against the United States.

The National Criminal Intelligence Sharing Plan is a formal intelligence sharing initiative that will securely link local, state, tribal, and federal law enforcement agencies, facilitating the exchange of critical intelligence information. The Plan contains model policies and standards and describes a nationwide communications capability that will link all levels of law enforcement personnel, including officers on the street, intelligence analysts, unit commanders, and police executives.





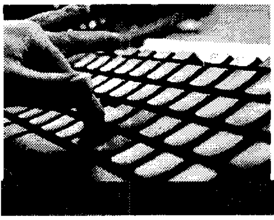
The National Criminal Intelligence Sharing Plan: why we need it, and how it got started

When President George W. Bush called for the creation of a Cabinet-level agency to coordinate homeland security, he emphasized improved criminal intelligence sharing as ***critical*** to enhancing law enforcement and other emergency agencies' abilities to protect the American public.

In fall 2001, law enforcement officers attending the International Association of Chiefs of Police (IACP) conference in Toronto, Canada, identified a need for an assessment to identify the inadequacies of the intelligence process that, in part, led to the failure to prevent the tragic events of September 11.

As a result, **law enforcement executives and intelligence experts joined resources at the IACP Criminal Intelligence Sharing Summit,** held in Alexandria, Virginia, in March 2002, and articulated a proposal for an intelligence-sharing plan that was in alignment with the President's initiative. They envisioned non-federal, law enforcement agencies fully participating with federal agencies to coordinate, collect, analyze, and appropriately disseminate criminal intelligence data across the United States, to make our nation safer.

> "*The need for intelligence sharing is paramount to our nation's safety. It is absolutely critical that we break down the barriers and expeditiously implement a plan for intelligence sharing that is continuously emphasized and built upon.*"
>
> **Joseph Polisar,**
> Chief of the Garden Grove (CA) Police Department and IACP first vice president



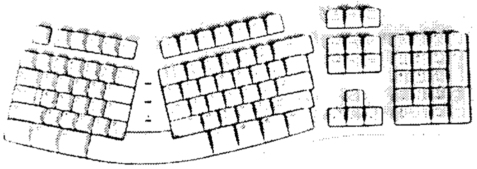
How is this collaboration achieved?

Summit participants called for the creation of some type of criminal intelligence coordinating council. As planned, this collective, comprised of all types of law enforcement agencies, would develop and oversee the National Criminal Intelligence Sharing Plan. Key to the process was efficient leveraging of existing efforts—the commitment to ***build on***, not reinvent substantial information sharing activities already underway.

Summit recommendations also included:

- Development of standardized policies, operating procedures, and training guidelines
- Creation of an outreach strategy
- Protection of individuals' civil rights

Additional information on the IACP Summit can be located in *Recommendations from the IACP Intelligence Summit, Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing at the Local, State and Federal Levels.* This document is available at http://www.theiacp.org/documents/pdfs/Publications/intelsharingreport.pdf.



The Global Intelligence Working Group (GIWG) is developing the National Criminal Intelligence Sharing Plan

In fall 2002, in response to this crucial need, the U.S. Department of Justice, Office of Justice Programs (OJP), Bureau of Justice Assistance (BJA), authorized the formation of the **Global Intelligence Working Group**, one of several issue-focused subgroups of the Global Justice Information Sharing Initiative Advisory Committee.[1]

The GIWG serves as the Criminal Intelligence Coordinating Council recommended by the IACP Summit participants.

The GIWG achieves comprehensive law enforcement and justice representation through participation from the following organizations and constituencies:

- Federal Bureau of Investigation (FBI)
- High Intensity Drug Trafficking Areas
- International Association of Chiefs of Police
- International Association of Law Enforcement Intelligence Analysts
- INTERPOL-USNCB
- Justice Management Institute
- Law Enforcement Intelligence Unit
- Local, state, and tribal police agencies[2]
- Major Cities Chiefs Association
- National Conference of State Legislatures
- National Sheriffs' Association
- National White Collar Crime Center
- Prosecutors
- Regional Information Sharing Systems
- State Law Enforcement Intelligence Networks
- U.S. Drug Enforcement Administration
- U.S. Department of Homeland Security
- U.S. Department of Justice

> "*Making the benefits of the National Criminal Intelligence Sharing Plan clear to patrol officers, detectives, intelligence unit managers, law enforcement executives, and federal officers is key to the GIWG vision.*"
>
> **Melvin Carraway,**
> Chairman of the GIWG
> and Superintendent of
> the Indiana State Police

[1] Global, operating under the auspices of BJA, serves as an advisory body to the federal government—specifically through the Assistant Attorney General, OJP, and the U.S. Attorney General—in facilitating standards-based electronic information exchange throughout the justice and public safety communities. The Global Advisory Committee (GAC or "Committee") is comprised of key personnel from local, state, tribal, federal, and international justice and public safety entities, and includes agency executives and policymakers; automation planners and managers; information practitioners; and, most importantly, end users. GAC membership reflects the fundamental Global tenet that the entire justice-interested community must be involved in information exchange. Global working groups, made up of committee members and other subject-matter experts, expand the GAC's knowledge and experience. These groups are formed around timely issues impacting justice information sharing; the GIWG is one of four working groups. For more information on Global, please visit http://www.it.ojp.gov/global/

[2] Local, state, and tribal law enforcement representatives are key participants and stakeholders in the development of this Plan. It is believed that their familiarity with local processes will contribute towards the Plan's successful implementation.

The Challenges for the GIWG

Members of the GIWG realize that challenges lie before them. They are committed to overcoming longstanding historical barriers hindering intelligence sharing, as well as future impediments that may develop. They acknowledge a major component will be informing all relevant communities of the existence of the National Criminal Intelligence Sharing Plan. Immediate acceptance of the Plan is not guaranteed. Ongoing training and education will be a major factor in the successful implementation and continuation of this National Criminal Intelligence Sharing Plan effort.

GIWG Mission Statement and Vision

The GIWG mission is to develop, build, and support the creation of the National Criminal Intelligence Sharing Plan, which will provide justice-related agencies with the ability to gather, analyze, protect, and share information and intelligence to identify, investigate, prevent, deter, and defeat criminal and terrorist activities, both domestically and internationally, as well as protect the security of our homeland and preserve the rights and freedoms of all Americans.

Using the above mission as a foundation to build upon, the GIWG members articulated a vision of what the National Criminal Intelligence Sharing Plan should be to local state, tribal, and federal law enforcement agencies:

- A model intelligence-sharing plan
- A mechanism to provide seamless sharing of information between systems
- A model for intelligence process principles and policies
- A national model for intelligence training
- An outreach model to promote intelligence sharing
- A model for protecting individuals' privacy and civil rights
- A blueprint for law enforcement administrators to follow when reviewing their own intelligence system or building a new one
- A mechanism to promote intelligence-led policing

When will the National Criminal Intelligence Sharing Plan be available?

The GIWG will provide an interim report containing preliminary recommendations for the Plan to BJA in May 2003. The final report is due in October 2003, and will be posted on the Global web site.

To best address the IACP Summit recommendations and realize tenets of the vision, the GIWG is divided into committees.

The GIWG committees have identified goals and associated tasks, including:

- Identifying necessary policies and frameworks for implementing standards-based intelligence sharing
- Identifying standards for collection, collation, storage, analysis, evaluation, and dissemination of intelligence information
- Ensuring compatibility of policies, standards, guidelines, and operating procedures of current and proposed sharing systems
- Ensuring individuals' privacy and civil rights are protected
- Development of an outreach plan to publicize and institutionalize the National Criminal Intelligence Sharing Plan
- Development of a training plan supporting all levels of law enforcement

> “*Imagine the ability to have access to a comprehensive document which would enable law enforcement officials to develop a new system utilizing established and proven policies and standards. The National Criminal Intelligence Sharing Plan will do that and more.*”
>
> **Bill Berger,**
> Chief of the North Miami Beach (FL) Police Department, and past IACP president

The GIWG understands that intelligence sharing cannot occur without trust between the parties sharing information. Thus, one of the central tasks of the GIWG is to increase communication, strengthen relationships, and help build trust between agencies and individuals in the intelligence network.

Melvin Carraway, Chairman of the GIWG and Superintendent of the Indiana State Police related, "The Intelligence Working Group is readily working on overcoming the impediments to intelligence sharing."

Why We Need the National Criminal Intelligence Sharing Plan

Have they finally caught him?

Imagine a detective working a fraud investigation and as a result of a ***single*** inquiry into a networked system—connected to local, state, regional, and federal databases—responses are received from the FBI and a state law enforcement agency that the subject is also a target of a major money laundering operation which may be supplying several terrorist organizations. The detective then contacts the intelligence analyst listed as the point of contact in the networked system, who provides a comprehensive briefing document that explains how the detective's fraud investigation fits into the "big picture."

Save time. Save money.
Create better intelligence systems.

Picture law enforcement executives preparing to develop an intelligence system. Instead of wading through a series of false starts, the executives have—at their fingertips—a source of established standards for managing intelligence data and ensuring system security. They will have access to established, proven model policies and standards that promote intelligence sharing, while ensuring individuals' rights to privacy.

Quality training for all.

Your staff could access quality intelligence training programs for all levels of personnel, regardless of the size or location of your law enforcement agency.

Is it too good to be true to have a single initiative addressing all these concerns? Not when the National Criminal Intelligence Sharing Plan is finalized and accepted.

For more information:

More information about the National Criminal Intelligence Sharing Plan or the GIWG can be obtained from the Global web site **www.it.ojp.gov/global**.

In addition, presentations and briefings regarding the National Criminal Intelligence Sharing Plan are anticipated at upcoming association and organizational meetings for groups such as the IACP, Law Enforcement Intelligence Unit, National Sheriffs' Association, Major Cities Chiefs Association, International Association of Law Enforcement Intelligence Analysts, and the National Organization of Black Law Enforcement Executives.