Executive Summary

National Criminal Intelligence Sharing Plan

United States Department of Justice

Reprinted 02/08

The need for a *National Criminal Intelligence Sharing Plan* ("Plan") was recognized as critical after the tragic events of September 11, 2001, when nearly 3,000 innocent lives were lost as a result of terrorist attacks against the United States. This event initiated a concerted effort by American law enforcement agencies to correct the inadequacies and barriers that impede information and intelligence sharing—so that future tragedies could be prevented.

In spring 2002, law enforcement executives and intelligence experts attending the International Association of Chiefs of Police (IACP) Criminal Intelligence Sharing Summit recognized that local, state, tribal, and federal law enforcement agencies and the organizations that represent them must work towards common goals—gathering information and producing intelligence within their agency and sharing that intelligence with other law enforcement and public safety agencies. Summit participants called for the creation of a nationally coordinated criminal intelligence council that would develop and oversee a national intelligence plan.[1] In response to this crucial need, the U.S. Department of Justice's Global Justice Information Sharing Initiative (Global) Intelligence Working Group (GIWG) was formed. Local, state, and tribal law enforcement representatives were key participants in the development of the *National Criminal Intelligence Sharing Plan*.

Many state law enforcement agencies and all federal agencies tasked with intelligence gathering and assessment responsibilities have established intelligence functions within their organizations. However, approximately 75 percent of the law enforcement agencies in the United States have less than 24 sworn officers, and more often than not, these agencies do not have staff dedicated to intelligence functions. Officers in these smaller, local agencies interact with the public in the communities they patrol on a daily basis. Providing local agencies with the tools and resources necessary for developing, gathering, accessing, receiving, and sharing intelligence information is critically important to improving public safety and homeland security.

During a February 2003 speech, President George W. Bush pledged to make information sharing an important tool in the nation's war on terror. "All across our country we'll be able to tie our terrorist information to local information banks so that the front line of defeating terror becomes activated and real, and those are the local law enforcement officials. We expect them to be a part of our effort; we must give them the tools necessary so they can do their job." The *National Criminal Intelligence Sharing Plan* is a key tool that law enforcement agencies can employ to support their crime-fighting and public safety efforts.

"This Plan represents law enforcement's commitment to take it upon itself to ensure that the dots are connected, be it in crime or terrorism. The Plan is the outcome of an unprecedented effort by law enforcement agencies, with the strong support of the Department of Justice, to strengthen the nation's security through better intelligence analysis and sharing."

Former U.S. Attorney General
John Ashcroft
May 14, 2004
National Kick-Off Event

[1] 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/intelshaingreport.pdf.

One of the key issues acknowledged by the GIWG was the need to overcome the long-standing and substantial barriers that hinder intelligence sharing.

Whether it is the officer on the street, the intelligence manager, or the agency executive—having access to the information that will help them do their job is essential. As law enforcement officials begin reviewing this Plan, they should ask themselves the questions, "What is my responsibility?" and "What can I do to get involved?" They should assess what type of intelligence functions are currently being performed in their agency and utilize the guidelines in this Plan to determine how they can improve their intelligence process.

This report outlines specific "action steps" that can be taken immediately by almost any agency and what can be expected by performing those steps. The portion of the Plan titled "The Rationale for the *National Criminal Intelligence Sharing Plan*" should be carefully reviewed, as it provides an in-depth discussion of the issues and recommendations presented in the *National Criminal Intelligence Sharing Plan*.

GIWG Vision

The GIWG membership 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 promote intelligence-led policing.
- A blueprint for law enforcement administrators to follow when enhancing or building an intelligence system.
- A model for intelligence process principles and policies.
- A plan that respects and protects individuals' privacy and civil rights.
- A technology architecture to provide secure, seamless sharing of information among systems.
- A national model for intelligence training.
- An outreach plan to promote timely and credible intelligence sharing.
- A plan that leverages existing systems and networks, yet allows flexibility for technology and process enhancements.

The GIWG focused its efforts on developing an intelligence sharing plan that emphasized better methods for developing and sharing critical data among all law enforcement agencies.

The GIWG identified several issues that were viewed as inhibitors of intelligence development and sharing. The GIWG expressed these issues as needs when formulating recommendations for the national plan. One of the key issues acknowledged by the GIWG was the need to **overcome the long-standing and substantial barriers that hinder intelligence sharing**. Examples include the "hierarchy" within the law enforcement and intelligence communities and deficits in intelligence. Overcoming the barriers that impede information and intelligence sharing is a continuous endeavor that will require a firm commitment by all levels of government, and the implementation of the *National Criminal Intelligence Sharing Plan* will most certainly assist in this undertaking.

The following additional issues were recognized and addressed by the GIWG:

- The need to develop minimum standards for management of an intelligence function.
- The need to establish a Criminal Intelligence Coordinating Council, composed of local, state, tribal, and federal entities, that will provide and promote a broadly inclusive criminal intelligence generation and sharing process.
- The need to ensure institutionalization of the *National Criminal Intelligence Sharing Plan*.
- The need to ensure that individuals' constitutional rights, civil liberties, civil rights, and privacy interests are protected throughout the intelligence process.
- The need to develop minimum standards for all levels of the intelligence process: Planning and Direction, Information Collection, Processing/Collation, Analysis, Dissemination, and Reevaluation (feedback).
- The need to increase availability of information, from classified systems to local and state law enforcement agencies, for the prevention and investigation of crime in their jurisdictions.
- The need to develop minimum criminal intelligence training standards for all affected levels of law enforcement personnel, to include training objectives, missions, number of hours, and frequency of training.
- The need to identify an intelligence information sharing capability that can be widely accessed by local, state, tribal, and federal law enforcement and public safety agencies.

From the issues identified above, the GIWG developed recommendations for the *National Criminal Intelligence Sharing Plan*. Following are the action items and steps that local, state, tribal, and federal law enforcement agencies should use as a road map to ensure that effective intelligence sharing becomes institutionalized throughout the law enforcement community nationwide.

This report represents the first version of the Plan that is intended to be a "living document" and that will be periodically updated. Those charged with developing and implementing the Plan will continue to solicit the involvement of the law enforcement and intelligence communities, national organizations, and other government and public safety entities, in order to ensure that the Plan is responsive to their needs for information and intelligence development and sharing.

Action Items/Recommendations

The primary purpose of intelligence-led policing is to provide public safety decision makers with the information they need to protect the lives of our citizens. The following recommendations detail the essential elements of the *National Criminal Intelligence Sharing Plan*.

Recommendation 1: In order to attain the goals outlined in this Plan, law enforcement agencies, regardless of size, shall adopt the minimum standards for intelligence-led policing and the utilization and/or management of an intelligence function as contained in the *National Criminal Intelligence Sharing Plan*. The standards focus on the intelligence process and include elements such as mission of the function, management and supervision, personnel selection, training, security, privacy rights, development and dissemination of intelligence products, and accountability measures.

The National Criminal Intelligence Sharing Plan—solutions and approaches for a cohesive plan to improve our nation's ability to develop and share criminal intelligence

The agency chief executive officer and the manager of intelligence functions should:

- Seek ways to enhance intelligence sharing efforts and foster information sharing by participating in task forces and state, regional, and federal information sharing initiatives.
- Implement a mission statement for the intelligence process within the agency.
- Define management and supervision of the function.
- Select qualified personnel for assignment to the function.
- Ensure that standards are developed concerning background investigations of staff/system users to ensure security (of the system, facilities, etc.) and access to the system/network.
- Ensure appropriate training for all personnel assigned to or impacted by the intelligence process.
- Ensure that individuals' privacy and constitutional rights are considered at all times.
- Support the development of sound, professional analytic products (intelligence).
- Implement a method/system for dissemination of information to appropriate components/entities.
- Implement a policies and procedures manual. The intent of the manual is to establish, in writing, agency accountability for the intelligence function. The manual should include policies and procedures covering all aspects of the intelligence process.
- Implement an appropriate audit or review process to ensure compliance with policies and procedures.
- Promote a policy of openness when communicating with the public and all interested parties regarding the criminal intelligence process, when it does not affect the security and integrity of the process.

Recommendation 2: In order to provide long-term oversight and assistance with the implementation and refinement of the *National Criminal Intelligence Sharing Plan*, a Criminal Intelligence Coordinating Council (CICC) should be established as contemplated in the IACP *Criminal Intelligence Sharing Report*. The purpose of the CICC is to advise the Congress, the U.S. Attorney General, and the Secretary of the U.S. Department of Homeland Security on the best use of criminal intelligence to keep our country safe. The CICC should operate under the auspices of the Global Advisory Committee (GAC). The CICC should consist of representatives from local, state, tribal, and federal agencies and national law enforcement organizations. The GIWG will act as the interim CICC until such time as the CICC is operational.

Recommendation 3: The CICC should monitor the implementation of the *National Criminal Intelligence Sharing Plan*, in order to gauge the success of the Plan. A report on the progress of the Plan will be submitted to the Office of Justice Programs (OJP) beginning December 31, 2004, and annually thereafter.

Recommendation 4: This Plan is designed to strengthen homeland security and foster intelligence-led policing. There is a critical need for more national funding to accomplish these goals. Without adequate funding, many of the recommendations contained herein, such as improving training and technical infrastructure, will not occur, and the country will remain at risk. The CICC, the GAC, and the U.S. Departments of Justice and Homeland Security should partner to identify and fund initiatives that implement the recommendations contained in this report.

Recommendation 5: In order to publicly recognize the creation of the Plan and demonstrate a commitment by all parties involved, a National Signing Event should be held where law enforcement and homeland security agency heads, from all levels, and other relevant groups come together to "sign on" to the *National Criminal Intelligence Sharing Plan*.

Recommendation 6: All parties involved with implementing and promoting the *National Criminal Intelligence Sharing Plan* should take steps to ensure that the law enforcement community protects individuals' privacy and constitutional rights within the intelligence process.

Recommendation 7: Local, state, tribal, and federal law enforcement agencies must recognize and partner with the public and private sectors in order to detect and prevent attacks to the nation's critical infrastructures. Steps should be taken to establish regular communications and methods of information exchange.

Recommendation 8: Outreach materials prepared by the CICC should be utilized by law enforcement agency officials to publicize and promote the concepts of standards-based intelligence sharing and intelligence-led policing, as contained within the *National Criminal Intelligence Sharing Plan*, to their agency personnel and the communities that they serve.

Recommendation 9: In order to ensure that the collection/submission, access, storage, and dissemination of criminal intelligence information conforms to the privacy and constitutional rights of individuals, groups, and organizations, law enforcement agencies shall adopt, at a minimum, the standards required by the Criminal Intelligence Systems Operating Policies federal regulation (28 CFR Part 23),[2] regardless of whether or not an intelligence system is federally funded.

Recommendation 10: Law enforcement agencies should use the IACP's *Criminal Intelligence Model Policy* (2003 revision)[3] as a guide when implementing or reviewing the intelligence function in their organizations.

Recommendation 11: In addition to federal regulation 28 CFR Part 23, law enforcement agencies should use the Law Enforcement Intelligence Unit (LEIU) *Criminal Intelligence File Guidelines* as a model for intelligence file maintenance.

Recommendation 12: The International Association of Law Enforcement Intelligence Analysts (IALEIA) should develop, on behalf of the CICC, minimum standards for intelligence analysis to ensure intelligence products are accurate, timely, factual, and relevant and recommend implementing policy and/or action(s).

---

[2]This 28 CFR Part 23 regulation is available at www.it.ojp.gov.
[3]The IACP *Criminal Intelligence Model Policy* is available at www.theiacp.org.

During a February 2003 speech, President George W. Bush pledged to make information sharing an important tool in the nation's war on terror.

Law enforcement agencies should adopt these standards as soon as developed and approved by the CICC.

Recommendation 13: To further enhance professional judgment, especially as it relates to the protection of individuals' privacy and constitutional rights, the *National Criminal Intelligence Sharing Plan* encourages participation in professional criminal intelligence organizations and supports intelligence training for all local, state, tribal, and federal law enforcement personnel.

Recommendation 14: To foster trust among law enforcement agencies, policymakers, and the communities they serve, the *National Criminal Intelligence Sharing Plan* promotes a policy of openness to the public regarding the criminal intelligence function, when it does not affect the security and integrity of the process.

Recommendation 15: The *National Criminal Intelligence Sharing Plan* promotes effective accountability measures, as expressed in 28 CFR Part 23, the LEIU *Criminal Intelligence File Guidelines*, and the *Justice Information Privacy Guideline*,[4] which law enforcement agencies should employ to ensure protection of individuals' privacy and constitutional rights and to identify and remedy practices that are inconsistent with policy.

Recommendation 16: Law enforcement agencies involved in criminal intelligence sharing are encouraged to use, to the extent applicable, the privacy policy guidelines provided in *Justice Information Privacy Guideline*: *Developing, Drafting and Assessing Privacy Policy for Justice Information Systems*. 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 (multiagency) justice systems.

Recommendation 17: The CICC, in conjunction with federal officials, should identify technical means to aid and expedite the production of unclassified "tear-line" reports. These reports are the declassification of classified data needed for law enforcement purposes, with the sensitive source and method-of-collection data redacted, yet retaining as much intelligence content as feasible.

Recommendation 18: Training should be provided to all levels of law enforcement personnel involved in the criminal intelligence process. The training standards, as contained within the *National Criminal Intelligence Sharing Plan*, shall be considered the minimum training standards for all affected personnel. 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 19: The CICC shall foster a working relationship with the International Association of Directors of Law Enforcement Standards and Training (IADLEST) organization, the IACP State and Provincial Police Academy Directors Section (SPPADS), and other relevant training organizations, in order to obtain

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

their assistance with implementing the recommended *National Criminal Intelligence Sharing Plan* training standards in every state.

Recommendation 20: In order to support agency tactical, operational, and strategic needs, law enforcement agencies are encouraged to consider an automated, incident-based criminal records tracking capability, in addition to traditional case management and intelligence systems, to use as an additional source for records management and statistical data. These systems should be Web-based and configured to meet the internal reporting and record-keeping needs of the component, in order to facilitate the exportation of desired data elements—without the need for duplicate data entry or reporting—to relevant statewide and federal criminal information programs.

Recommendation 21: The Regional Information Sharing Systems® (RISS) and the Federal Bureau of Investigation (FBI) Law Enforcement Online (LEO) systems, which interconnected September 1, 2002, as a virtual single system, shall provide the initial sensitive but unclassified secure communications backbone for implementation of a nationwide criminal intelligence sharing capability. This nationwide sensitive but unclassified communications backbone shall support fully functional, bidirectional information sharing capabilities that maximize the reuse of existing local, state, tribal, regional, and federal infrastructure investments. Further configuration of the nationwide sensitive but unclassified communications capability will continue to evolve in conjunction with industry and the development of additional standards and the connection of other existing sensitive but unclassified networks.

Recommendation 22: Interoperability with existing systems at the local, state, tribal, regional, and federal levels with the RISS/LEO communications capability should proceed immediately, in order to leverage information sharing systems and expand intelligence sharing.

Recommendation 23: The CICC shall work with Global's Systems Security Compatibility Task Force to identify and specify an architectural approach and transitional steps that allow for the use of existing infrastructures (technology, governance structures, and trust relationships) at the local, state, tribal, regional, and federal levels, to leverage the national sensitive but unclassified communications capabilities for information sharing. This strategic architectural approach shall ensure interoperability among local, state, tribal, regional, and federal intelligence information systems and repositories.

Recommendation 24: All agencies, organizations, and programs with a vested interest in sharing criminal intelligence should actively recruit agencies with local, state, tribal, regional, and federal law enforcement and intelligence systems to connect to the nationwide sensitive but unclassified communications capability. Such agencies, organizations, and programs are encouraged to leverage the nationwide sensitive but unclassified communications capability, thereby expanding collaboration and information sharing opportunities across existing enterprises and leveraging existing users. Moreover, participant standards and user vetting procedures must be compatible with those of the currently connected sensitive but unclassified systems, so as to be trusted connections to the nationwide sensitive but unclassified communications capability.

Recommendation 25: Agencies participating in the *National Criminal Intelligence Sharing Plan* are encouraged to use *Applying Security Practices to Justice Information Sharing*[5] as a reference document regarding information system security practices. The document was developed by the Global Security Working Group 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.

Recommendation 26: Agencies are encouraged to utilize the latest version of the Global Justice Extensible Markup Language (XML) Data Model (Global JXDM) and its component Global Justice XML Data Dictionary (Global JXDD)[6] when connecting databases and other resources to communication networks. The Global JXDM and Global JXDD were developed to enable interoperability through the exchange of data across a broad range of disparate information systems.

Recommendation 27: In order to enhance trust and "raise the bar" on the background investigations currently performed, law enforcement agencies must conduct fingerprint-based background checks on individuals, both sworn or nonsworn, prior to allowing law enforcement access to the sensitive but unclassified communications capability. Background requirements for access to the nationwide sensitive but unclassified communications capability by law enforcement personnel shall be consistent with requirements applied to the designation and employment of sworn personnel, as set by the participating state or tribal government, so long as, at a minimum, those requirements stipulate that a criminal history check be made through the FBI and the appropriate local, state, and tribal criminal history repositories and be confirmed by an applicant fingerprint card. Additionally, a name-based records check must be performed on law enforcement personnel every three years after the initial fingerprint-based records check is performed.

Recommendation 28: The CICC, in conjunction with OJP and the connected sensitive but unclassified systems, shall develop an acquisition mechanism or centralized site that will enable law enforcement agencies to access shared data visualization and analytic tools. The CICC shall identify analytical products that are recommended for use by law enforcement agencies in order to maximize resources when performing intelligence functions, as well as a resource list of current users of the products.

---

[5]This document is available at http://www.it.ojp.gov/global/.
[6]The latest version of the Global JXDM and the Global JXDD can be found at http://www.it.ojp.gov/jxdm.

For more information on Global, please visit www.it.ojp.gov/global/.

BJA This document was prepared under the leadership, guidance, and funding of the Bureau of Justice Assistance (BJA), Office of Justice Programs, U.S. Department of Justice, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative. The opinions, findings, and conclusions or recommendations expressed in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.