United States
Department of Justice

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

October 2003

United States
Department of Justice

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

October 2003

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.

This project was supported by Award No. 2000-LD-BX-0003, awarded by the Office of Justice Programs.

Table of Contents

Executive Summary

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 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*.

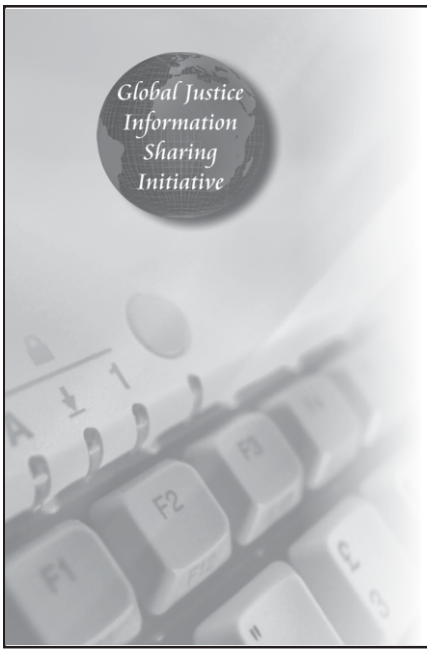
Many state law enforcement agencies and all federal agencies tasked with intelligence gathering and assessment responsibilities have established intelligence functions within their organizations. However, approximately 75 percent of the law enforcement agencies in the United States have less than 24 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.

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 report 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*.

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/intelsharingreport.pdf.



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 their 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 t**o 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, which is intended to be a "living document," and 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 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 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*. The National Signing Event should be held before December 31, 2003.

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.[4]

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). These minimum standards should be developed by June 30, 2004. 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*,[5] 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*.[6] 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. The technical means for production of these reports should be identified by June 30, 2004.

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

2 This 28 CFR Part 23 regulation is included on the companion CD and is also available at www.it.ojp.gov.

3 The IACP *Criminal Intelligence Model Policy* is included on the companion CD and is also available at www.theiacp.org.

4 The March 2002 update of the LEIU *Criminal Intelligence File Guidelines* is included on the companion CD.

5 This document is included on the companion CD and is also available at: http://www.ncja.org/pdf/privacyguideline.pdf.

6 This document is available at http://www.ncja.org/pdf/privacyguideline.pdf.

7 The recommended training standards for each level, including roles and missions, core training objectives, and length of training, are included in the appendix of this report and on the companion CD.

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.[8]

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*[9] as a reference document regarding information system security practices. The document was developed by the Global Security Working Group (GSWG) 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)[10] 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.

8 The GIWG conducted a preliminary survey of systems/initiatives that are operational or being developed at the local, state, regional, and federal levels. Several systems/initiatives were identified. Refer to the companion CD for a list of the systems identified, as well as summary information obtained during the survey.

9 This document is available at: http://www.it.ojp.gov/global/.

10 The latest version of the Global Justice XML Data Model and the Global Justice XML Data Dictionary is included on the companion CD and can be found at: http://www.it.ojp.gov/jxdm.

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. The CICC will submit a report on these tools to OJP by June 30, 2004.

Acknowledgements

The GIWG wishes to acknowledge the following GIWG members for their dedication and tireless efforts towards the completion of this document:

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

Mr. Kenneth Bouche
Illinois State Police
Chicago, Illinois

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. Steve Casteel
U.S. Drug Enforcement Administration
Arlington, Virginia

Mr. Henry Coffman
INTERPOL-USNCB
Washington, DC

Mr. David Cohen
New York City, New York, Police Department
New York, New York

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

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

Mr. Max Fratoddi
Federal Bureau of Investigation
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
Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network®
Newtown, Pennsylvania

Mr. George P. March
Office of Information Technology
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
National Drug Intelligence Center
Johnstown, Pennsylvania

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. 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. Secret Service
U.S. Department of Homeland Security
Washington, DC

Mr. Richard H. Ward III (Retired)
Bureau of Justice Assistance
Washington, DC

The GIWG would also like to acknowledge the following individuals for their contributions to this document:

Ms. Maureen Baginski
Federal Bureau of Investigation
Washington, DC

Mr. Jim Burch
Bureau of Justice Assistance
Washington, DC

Mr. David Clopton
System Planning Corporation
Arlington, Virginia

Mr. Bruce Edwards
Bureau of Justice Assistance
Washington, DC

Mr. John Elliff
Federal Bureau of Investigation
Washington, DC

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

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

Mr. Cliff Karchmer
Police Executive Research Forum
Washington, DC

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

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

Mr. Steve McCraw
Federal Bureau of Investigation
Washington, DC

Dr. John Morgan
National Institute of Justice
Washington, DC

Ms. Karen Morr
U.S. Department of Homeland Security
Washington, DC

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

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

Mr. Kevin Perham
New York City, New York, Police Department
Brooklyn, New York

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

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

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

Mr. Craig Samtmann
Federal Bureau of Investigation
Washington, DC

Mr. Mike Sapsara
U.S. Drug Enforcement Administration
Miami, Florida

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

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

Mr. Kenneth Staab
Broward County, Florida, Sheriff's Office
Pompano Beach, Florida

Mr. Len Starling
Federal Bureau of Investigation
Washington, DC

Mr. Mark Tanner
Federal Bureau of Investigation
Washington, DC

Ms. Kathleen Timmons
Federal Bureau of Investigation
Washington, DC

Mr. David Walchak
Federal Bureau of Investigation
Washington, DC

The Rationale for the *National Criminal Intelligence Sharing Plan*

Background and Methodology

Convening the International Association of Chiefs of Police (IACP) Criminal Intelligence Sharing Summit

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 law enforcement 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 President Bush'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*.[11]

The IACP *Criminal Intelligence Sharing Report* contained a proposal to create the *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 (CICC or "Council") composed of local, state, tribal, and federal law enforcement executives.[12] 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.

The IACP Summit participants noted that the Plan and the CICC's mandate must overcome the barriers that hinder intelligence sharing. The following barriers were identified as some of the most significant: the absence of a nationally coordinated process for intelligence generation and sharing; the "hierarchy" within the law enforcement and intelligence communities; local, state, tribal, and federal laws and policies that unduly restrict law enforcement access to information; the inaccessibility and/or disaggregation of technologies to support intelligence sharing; and deficits in analysis.

Formation of the Global Intelligence Working Group

In fall 2002, in response to the IACP's proposal to create the *National Criminal Intelligence Sharing Plan*, the U.S. Department of Justice (DOJ), Office of Justice Programs (OJP), authorized the formation of the Global Justice

11 This document is available at: http://www.theiacp.org/documents/pdfs/Publications/intelsharingreport.pdf.
12 IACP *Criminal Intelligence Sharing Report*, p. 6.

Information Sharing Initiative (Global) Intelligence Working Group (GIWG), one of several issue-focused working groups of the Global Advisory Committee (GAC).[13] 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 OJP, in consultation with the Global Executive Steering Committee, based on their backgrounds and broad experiences with criminal justice and criminal intelligence issues. These officials represented all levels of law enforcement, including practitioners, policymakers, and subject-matter experts. In addition to local, state, tribal, regional, and federal law enforcement personnel, the individuals on the GIWG represent the following organizations and groups: Counterdrug Intelligence Executive Secretariat (CDX); Criminal Information Sharing Alliance (CISA); IACP; International Association of Law Enforcement Intelligence Analysts (IALEIA); Justice Management Institute; Law Enforcement Intelligence Unit (LEIU); Major Cities Chiefs Association; National Conference of State Legislatures; National Drug Intelligence Center; National White Collar Crime Center (NW3C); National Sheriffs' Association (NSA); prosecutors; Regional Information Sharing Systems (RISS); SEARCH, The National Consortium of Justice Information and Statistics; and state Law Enforcement Intelligence Networks (LEIN).

GIWG's Mission and Vision

The GIWG members developed the following mission statement to formalize their intent to create the *National Criminal Intelligence Sharing Plan*:

> *The GIWG mission is to develop, build, and support the creation of the National Criminal Intelligence Sharing Plan, which will provide law enforcement agencies with the ability to gather, analyze, protect, and share credible and timely 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 statement 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 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.

Chairman Carraway established the following committees to fulfill the GIWG mission and vision and to address the goals and objectives outlined in the IACP *Criminal Intelligence Sharing Report*:

- **Connectivity/Systems Committee**, chaired by M. Miles Matthews, Executive Officer, CDX
- **Outreach Committee**, chaired by William Berger, Chief, North Miami Beach, Florida, Police Department and past IACP president
- **Policy Committee**, chaired by Thomas Frazier, Executive Director, 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
- **Training Committee**, chaired by Thomas O'Connor, Chief, Maryland Heights, Missouri, Police Department

After the initial gathering in Atlanta, the GIWG members convened four additional meetings to develop recommendations for the *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 presents the issues and recommendations formulated as a result of the GIWG committees' discussions, deliberations, and collaborations. This report contains and serves as the supporting documentation for the *National Criminal Intelligence Sharing Plan*.

13 The Global Justice Information Sharing Initiative (Global), operating under the program management of the Office of Justice Programs (OJP), serves as an advisory body to the federal government—specifically through the U.S. Attorney General and the Assistant Attorney General, OJP—to facilitate standards-based electronic information exchange throughout the justice and public safety communities. The Global Advisory Committee (GAC) 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, consisting 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 Global Intelligence Working Group is one of four working groups. For additional information on Global, please visit http://www.it.ojp.gov/global/.

Building on Existing Information

The IACP *Criminal Intelligence Sharing Report* recommendations were utilized as a blueprint by the GIWG when developing recommendations for the *National Criminal Intelligence Sharing Plan*. In addition to the IACP recommendations, other information was used, including a survey recently sponsored by the Major Cities Chiefs Association in which they requested survey respondents to provide the top five impediments to the flow of intelligence information between law enforcement agencies, which, if remedied, would most assist the agencies' investigative, enforcement, and prevention efforts. Surveys were distributed to all major cities' chiefs and sheriffs and heads of state-level law enforcement agencies. Preliminary findings suggest that the results are consistent with the barriers identified by the IACP Summit participants. The following are the top five impediments identified from the survey:

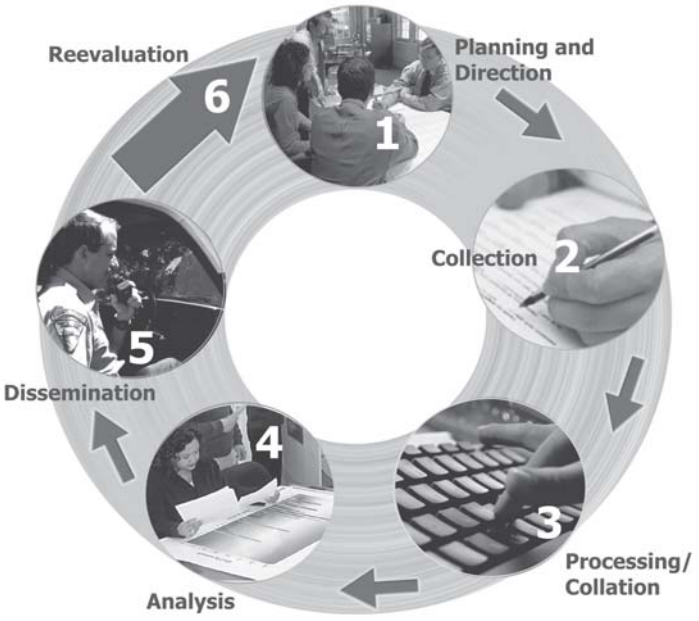
1. Lack of communication and information sharing—specifically, lack of a centralized analysis and dissemination function, either at the state or federal level; lack of intelligence from federal agencies; and state statutory requirements that present hurdles to sharing information.
2. Technology issues—specifically, lack of equipment to facilitate a national intelligence data system, lack of interconnectibility of law enforcement and other databases (e.g., immigration services), limited fiscal resources, lack of technological infrastructure throughout the state, and lack of uniformity between computer systems.
3. Lack of intelligence standards and policies—specifically, lack of common standards for collection, retention, and dissemination of intelligence data; a need for increased local training on legal standards for collection, storage, and purging of data; access to classified data; and lack of standards for determining when to disseminate intelligence to federal agencies.
4. Lack of intelligence analysis—specifically, lack of compatible analytical software and lack of analytical support, personnel, equipment, and training.
5. Poor working relationships—specifically, unwillingness of law enforcement agencies to provide information due to parochial interests and a culture within the federal system that does not foster sharing of information or trust between agencies.

In May 2003, preliminary recommendations for the Plan were developed and published in the GIWG's Interim Report. The preliminary recommendations were made available to the GIWG member organizations, to the public via Internet Web sites, and to various law enforcement groups, such as the annual conference of the LEIU in Seattle, Washington, in June 2003. Feedback on the preliminary recommendations was solicited, and the input was used to refine the recommendations.

The Importance of Criminal Intelligence, Intelligence-Led Policing, and Community Policing

The GIWG focused their efforts on developing an intelligence gathering and sharing plan that emphasizes better methods for sharing among all agencies and 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 reinvent, substantial information sharing activities already under way. As indicated by IACP Summit participants, it is difficult to enhance intelligence sharing without also having a common understanding of the phrase "criminal intelligence." IACP Summit participants noted that criminal intelligence is the combination of credible information with quality analysis information that has been evaluated and used to draw conclusions. Criminal intelligence results from a process involving planning and direction, information collection, processing/collation, analysis, dissemination, and reevaluation (feedback) of information on suspected criminals and/or organizations. This sequential process is commonly referred to as the intelligence process, and it will be further explained later in this document. The following graphic depicts this step-by-step process:

Intelligence Process



A recommendation that the IACP Summit participants identified as core to achieving the goals of the *National Criminal Intelligence Sharing Plan* was to "promote intelligence-led policing through a common understanding of criminal intelligence and its usefulness." Intelligence-led policing is defined as *the collection and analysis of information to produce*

an intelligence end product designed to inform law enforcement 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 philosophy, policies, and strategies and must also be integral in the organization's mission and goals.

Consistent with the IACP Summit findings and recommendations, GIWG members recognized the importance of community-oriented policing (COP) efforts when developing the national intelligence sharing plan. "Over the past decade, simultaneous to federally led initiatives to improve intelligence gathering, thousands of community-policing officers have been building close and productive relationships with the citizens they serve. The benefits of these relationships are directly related to information and intelligence sharing: COP officers have immediate and unfettered access to local, neighborhood information as it develops. Citizens are aware of and seek out COP officers to provide them with new information that may be useful to criminal interdiction or long-term problem solving. The positive nature of COP/citizen relationships promotes a continuous and reliable transfer of information from one to the other. It is time to maximize the potential for community-policing efforts to serve as a gateway of locally based information to prevent terrorism, and all other crimes."[14]

Recognition of Needs

A key need and goal identified by the GIWG was to ensure that the guiding principles contained within the *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 multifaceted and ongoing manner. The GIWG members envisioned that implementation of the Plan will provide the impetus for many law enforcement agencies to institute intelligence-led policing, which will help to substantially increase intelligence development and sharing, ultimately improving public safety.

GIWG members recognize that 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. Key elements of the Plan that will aid in this effort include model policies and standards for all law enforcement agencies to emulate; guidelines for local law enforcement to develop an intelligence function within their agency; access to analytic resources and tools previously unavailable; comprehensive training provision and outreach mechanisms, both of which provide education and continued emphasis on intelligence sharing; access to a nationwide network with links to local, state, tribal, regional, and federal databases; and implementation of security requirements that institute trust in network participants.

As indicated above, the GIWG identified several issues that were viewed as inhibitors to intelligence development and sharing. These issues are expressed as needs in this document. The GIWG then developed recommendations that are the steps to be taken to respond to these needs. The recommendations are explained in the section, "Recommendations for Implementation of the Plan," and the issues are explained below:

The need to develop minimum standards for management of an intelligence function.

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

14 IACP Criminal Intelligence Sharing Report, p. 2.

intelligence function can have a tremendous impact on a law enforcement agency and the community it serves.

As these enhanced capabilities are built, so, too, must proper management principles be implemented. Informal surveys during analytic training indicate that the primary reason agencies do not use analysis and intelligence is that the executives, managers, and supervisors of the function do not understand its capabilities and have not been given guidance in its use. Some guidance on management was provided in government publications in the 1970s[15] and in the 2001 version of the book *Intelligence 2000: Revising the Basic Elements*. This guidance, however, has not been universally disseminated or adopted.

Refer to Recommendation 1 for details and further discussion regarding this issue.

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 most central and enduring element of the *National Criminal Intelligence Sharing Plan* advocated by the IACP Summit participants was the call for a CICC. The Summit participants viewed the CICC 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.[16]

Refer to Recommendation 2 for details and further discussion regarding this issue.

The need to ensure institutionalization of the *National Criminal Intelligence Sharing Plan*.

Experience in law enforcement has shown that progress does not occur when a new philosophy of policing is adopted by a specific unit in law enforcement agencies rather than accepted universally by all units within the agencies. Thus, there is a need to institutionalize the use of intelligence and the *National Criminal Intelligence Sharing Plan* into the operations of all law enforcement agencies.

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. Providing credible and reliable intelligence to the agency in need is imperative to addressing criminal and terrorist activities. Whether it be the officer on the street, the intelligence manager, or the agency executive—having the information that will help them do their jobs is essential. The *National Criminal Intelligence Sharing Plan* will be a comprehensive reference document that every law enforcement officer should access when developing a plan to implement or enhance the intelligence process in his or her organization.

Refer to Recommendations 3, 4, 5, 7, 8, and 17 for details and further discussion regarding this issue.

The need to ensure that individuals' constitutional rights, civil liberties, civil rights, and privacy interests are protected throughout the intelligence process.

The protection of individuals' privacy and constitutional rights is an obligation of government officials and is crucial to the long-term 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.

For the purposes of this document, the term *constitutional rights* refers to those rights that an individual derives from the Constitution of the United States. Constitutional rights are the strongest protection from improper government conduct against an individual. Unlike other legal rights, constitutional rights cannot be changed by a statute. They can only be altered by amending the Constitution.

The term *civil liberties* refers to fundamental individual rights such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights—the first ten Amendments—to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference in relation to the specific freedoms enumerated in the Bill of Rights.

The term *civil rights* is used to imply that the state has a role in ensuring all citizens have equal protection under the law

15 Harris, Don R. and E. Drexel Godfrey, 1971. *The Basic Elements of Intelligence*, Washington, DC: U.S. Government Printing Office, and Don R. Harris, et al., *Basic Elements of Intelligence – Revised*, Washington, DC: Law Enforcement Assistance Administration.

16 IACP *Criminal Intelligence Sharing Report*, p. 2.

and equal opportunity to exercise the privileges of citizenship regardless of race, religion, sex, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed upon government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress. Generally, the term *civil rights* involves positive (or affirmative) government action, while the term *civil liberties* involves restrictions on government.

The term *privacy* refers to individuals' 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. The U.S. Constitution does not explicitly use the word *privacy*, but several of its provisions protect different aspects of this fundamental right.[17] Although there does not exist an explicit federal constitutional right to an individual's privacy,[18] privacy rights have been articulated in limited contexts by the U.S. Supreme Court.[19] Privacy protections are numerous and include protection from unnecessary or unauthorized collection of personal information (e.g., eavesdropping), public disclosure of private facts, and shame or humiliation caused by release of personal information.

The *National Criminal Intelligence Sharing Plan* supports policies that will protect privacy and constitutional rights while not hindering the intelligence process. When agencies are reviewing or formulating their policies, it may be helpful to view the intelligence process as a series of discretionary decisions.[20] At each step, a decision must be made, usually involving a choice from among several possible alternatives. Consider, for example, how a criminal intelligence unit might respond to an unsolicited, anonymous tip alleging that a particular individual is engaged in criminal activity. Should the unit query various police records systems in an effort to learn more about the "suspect"? Should they query commercial or other public record databases? Should they conduct surveillance of the "suspect"? Or should they disseminate the information to other law enforcement agencies in an effort to learn more about the person? What kinds of additional records are created when these actions are taken? And then, after those actions are taken, additional decisions must be made regarding what information and how much, if any, to store about the "suspect" in the criminal intelligence files. Violations of privacy and constitutional rights may potentially occur when choices are selected from these various alternatives. In order to be effective, a policy that addresses the protection of individual privacy and constitutional rights should attempt to eliminate the unnecessary discretion in the decision-making process, guide the necessary discretion, and continually audit the process to ensure conformance with the policy goals.[21]

It is imperative that a privacy policy have legitimacy; therefore, when an agency is developing a new policy or reviewing existing ones, interested parties and competing viewpoints should be represented. Legitimate parties include not only a wide selection of law enforcement agencies but also representatives from privacy and constitutional rights advocacy groups. Input from all interested parties is a vital step towards establishing legitimacy of the policy and achieving its widespread acceptance.

It is also essential that the parameters of a privacy policy be clearly defined. This includes, for example, identifying the particular aspects of the intelligence process to which it applies, as well as defining the scope and meaning of the phrase "individuals' privacy and constitutional rights." The extent to which information and activities have been held to be private or constitutionally protected under the law is, in all likelihood, much narrower than what the general public believes to be private and protected. This phenomenon must be understood and acknowledged when developing and conducting outreach in regards to these issues.

It is impossible for a policy to conceive of every imaginable situation or set of circumstances. An agency's privacy policy should, however, acknowledge and address important issues that currently are not included in some existing criminal intelligence policies. For example, the policy should acknowledge the existence of information that is received or possessed by law enforcement agencies that does not rise to the level of "reasonable suspicion of criminal activity" and provide guidance on how to process that information. Often this information—sometimes referred to as "temporary" or "working" files—is received unsolicited by law enforcement agencies and cannot simply be dismissed.

Finally, an agency's privacy policy should identify the decision points within the intelligence process and provide appropriate guidance and structure for each. This should be the heart of the policy—to map out clearly, for law enforcement personnel,

17 For early references to this principle, see Samuel Warren and Louis Brandeis. 1890 (December 15). "The Right to Privacy." *Harvard Law Review* 4(5): 193-220.

18 The most closely related constitutional right is that under the Fourth Amendment, which prohibits unreasonable search and seizure of individuals and their houses, papers, and effects. U.S. Constitution Amendment IV. Some states, such as California, recognize a right to privacy in their state constitutions. See California Constitution article 1, §1 (West 1983).

19 National Criminal Justice Association. 2002 (September). *Justice Information Privacy Guideline: Developing, Drafting and Assessing Privacy Policy for Justice Information Systems*. Washington, DC: NCJA, pp. 18-19.

20 This framework was used by Wayne LaFave, who observed, "It is helpful to look at the total criminal justice system as a series of interrelated discretionary choices." (LaFave, 1965). *Arrest*. Boston, MA: Little Brown. Like any model or framework, it is valuable not because it is the only way or the right way to describe the process, but because of the insights that it provides.

21 The framework for regulating discretionary decisions (i.e., eliminating unnecessary discretion and confining, structuring, and checking necessary discretion) through administrative rule making and agency policies is derived from Kenneth Culp Davis. (Davis, 1971). *Discretionary Justice: A Preliminary Inquiry*. Urbana, IL: University of Illinois; and (Davis, 1975). *Police Discretion*. St. Paul, MN: West Publishing Company.

the parameters of the decisions they must make throughout the intelligence process; educate them on permissible options; and provide guidance on appropriate choices. For example, the policy should stress the need for and importance of planning and direction (the first stage of the intelligence process). Although it is only one phase of the intelligence process, planning and direction guides the overall activities of the criminal intelligence function. Some of the most egregious violations of sound criminal intelligence practice can be prevented by developing a clear statement of the mission and goals of the criminal intelligence unit (usually in terms of crimes it seeks to prevent or investigate), establishing clear policies and procedures, appropriately tasking personnel, and performing ongoing checks to ensure that the criminal intelligence function is being carried out in accordance with this guidance.[22] As mentioned earlier, in addition to the decision points identified with the planning and direction phase of the intelligence process, discretionary decisions related to other phases of the intelligence process should also be specified, along with helpful guidance for each.[23]

Refer to Recommendations 6, 13, 14, 15, and 16 for details and further discussion regarding this issue.

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 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. There are various models of the intelligence process in use; however, most models contain the following basic steps: planning and direction, information collection, processing/collation, analysis, dissemination, and reevaluation (feedback). Storage and retention are additional steps that can be included.

The intelligence process (or cycle) is the means of developing raw information into finished intelligence products for use in decision making and formulating policies/actions. The first step, planning and direction, involves identifying the need for data. Agency members should engage in a process of deciding what they want to know (or what they need to collect) before they collect it, or they may end up with indiscriminate, unfocused information.

Collection is the gathering of the raw data needed to produce intelligence products. Data may be collected from many sources, including but not limited to public records, the Internet, confidential sources, incident reports, and periodicals.

The next step, processing and collation, involves evaluating the information's validity and reliability. Collation entails sorting, combining, categorizing, and arranging the data collected so relationships can be determined.

Analysis is the portion of the intelligence process that transforms the raw data into products that are useful. This is also the function that separates "information" from "intelligence." It is this vital function that makes the collection effort beneficial. Without this portion of the process, we are left with disjointed pieces of information to which no meaning has been attached. The goal is to develop a report where the information has been connected in a logical and valid manner to produce an intelligence report that contains valid judgments based on information analyzed.[24]

Dissemination is also a vital step in the process. Without disseminating the intelligence developed, it is pointless to collect it. The intelligence disseminated must be timely and credible to be useful. Dissemination must also be evaluated based on a "right to know" and the "need to know." The right to know means the recipient has the legal authority to obtain the information pursuant to court order, statute, or decisional law. The need to know means the requestor has the need to obtain information to execute official responsibilities.[25]

The final step of the intelligence process involves obtaining feedback on the process performed and the products produced by the intelligence function. This step allows evaluation of the performance or effectiveness of an intelligence function.

The proper completion of these steps ensures that the data used are managed appropriately and within the legal constraints regarding the privacy and rights of all citizens; however, the steps are often interconnected, and frequently, the boundaries blur. Each step of the process needs to be understood to produce accurate, timely intelligence reports.

The two primary standards applying to the intelligence process within the United States have been the Criminal Intelligence Systems Operating Policies 28 Code of Federal Regulations (CFR) Part 23 and the LEIU *Criminal Intelligence File*

22 For reference on the management of the criminal intelligence function, see: Wright, Richard. 2002. "Management of the Intelligence Unit." In Marilyn B. Peterson (Managing Ed.), Bob Morehouse and Richard Wright (Eds.), *Intelligence 2000: Revising the Basic Elements*. Sacramento, CA: Law Enforcement Intelligence Unit, and Lawrenceville, NJ: International Association of Law Enforcement Intelligence Analysts, Inc., pp. 67-77.

23 The GIWG would like to extend particular thanks to Special Agent in Charge Russ Porter of the Iowa Department of Public Safety for his contributions to the Plan regarding privacy issues and recommendations.

24 Morehouse, Bob. 2000. "The Role of Criminal Intelligence in Law Enforcement." In Marilyn B. Peterson (Managing Ed.), Bob Morehouse, and Richard Wright (Eds.), *Intelligence 2000: Revising the Basic Elements*, Sacramento, CA: Law Enforcement Intelligence Unit, and Lawrenceville, NJ: International Association of Law Enforcement Intelligence Analysts, Inc., pp. 1-12.

25 Ibid, p. 9.

Guidelines. Federal regulation 28 CFR Part 23 governs only those agencies that receive federal funding in support of a multijurisdictional intelligence system, while LEIU *File Guidelines* historically have applied only to its member agencies. Moreover, in the past, many agencies covered by these standards have only applied them to information given to or received from/through the multijurisdictional information system; thus, their other files might not be in compliance with these guidelines.

Refer to Recommendations 9, 10, 11, and 12 for details and further discussion regarding this issue.

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 IACP *Criminal Intelligence Sharing Report* noted the difficulties of intelligence sharing between local, state, tribal, and federal law enforcement agencies. The current laws, policies, and procedures that govern the classification of intelligence information and individuals' clearance to view data, as well as the length of time it takes to process security clearances, are examples that impede the transfer of intelligence between law enforcement agencies. The fact that some information needs to be classified is not disputed; however, the current process needs to become more efficient to better serve public safety and homeland defense.

Many local law enforcement agencies are expanding their intelligence functions, and many have personnel assigned to a Joint Terrorism Task Force (JTTF). Being a member of a JTTF requires a national security clearance of at least "secret" classification. A classification level is assigned to information owned by, produced by or for, or controlled by the United States government. Clearance levels are based on the need-to-know doctrine, which requires a background check for officials who need to have access to national security information. Information may be classified at one of the following levels:

1. "Top secret" is applied to information of which the unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security.
2. "Secret" is applied to information of which the unauthorized disclosure could reasonably be expected to cause serious damage to the national security.
3. "Confidential" is applied to information of which the unauthorized disclosure could reasonably be expected to cause damage to the national security.

Information is considered for classification if it concerns military plans, weapons systems, or operations; foreign government information; intelligence activities (including special activities), intelligence sources or methods, or cryptology; foreign relations or foreign activities of the United States, including confidential sources; scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism; United States government programs for safeguarding nuclear materials or facilities; vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or weapons of mass destruction.

The Federal Bureau of Investigation (FBI) brochure *Security Clearance Process for State and Local Law Enforcement* (2002) identifies two categories of clearance levels: a "secret" security clearance may be granted to those persons who have a need to know national security information that has been classified as "confidential" or "secret," and a "top secret" clearance may be granted to those persons who have a need to know national security information, classified up to the "top secret" level, and who need unescorted access in FBI facilities when necessary. The time required to obtain a "top secret" clearance is six to nine months. A "secret" clearance can be awarded in 45 days.

Presidential Executive Order mandates the background investigation and records checks for "secret" and "top secret" security clearances; the FBI does not have the ability to waive them. Local and state officials who require access to classified material must apply for security clearance through their local FBI field office. Understanding the inherent delays in such background checks, local officials should begin the application process promptly to help ensure a timely turnaround by federal officials.

Refer to Recommendations 4 and 17 for details and further discussion regarding this issue.

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 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.

Refer to Recommendations 18 and 19 for details and further discussion regarding this issue.

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.

Information and intelligence sharing is essentially a voluntary endeavor, whether in law enforcement, other areas of government, or the private sector. Certainly, policies exist to exhort, promote, and "require" information sharing. These may be expressed informally; assumed to be necessary and understood; or set down formally in the form of a written policy, memorandum of understanding, or statute.

Still, sharing is founded upon trust between the information provider and the intelligence consumer. Such trust is most often fostered on an interpersonal basis; therefore, law enforcement task forces and other joint work endeavors succeed where colocated, interspersed personnel from different agencies and job types convene for a common purpose. In these instances, sharing can either flourish or falter due to changes in leadership, personality differences, and real or perceived issues.

Trust is fostered and may be further institutionalized by setting standards for participation in the information sharing process; thus, personnel vetting procedures are established that range from the most stringent—national security clearances for access to classified information through law enforcement agencies' employment background checks, including criminal history records and indices—to situational criteria that define an individual's "need to know."

The IACP *Criminal Intelligence Sharing Report* correctly observed, "Technology cannot stand in for trust." However, technology systems can extend trust-building opportunities and facilitate collaboration well beyond the boundaries of direct interpersonal contact. Technical systems owners stipulate membership criteria; information owners define the criteria by which their systems or databases grant information access privileges. These are enforced through membership and access vetting procedures that serve to define and support trust relationships.

Technical systems provide a range of depth and breadth of information sharing, from almost full and unfettered access to another's collection of sensitive information through redacted reports that provide the gist of salient information while removing (and thus further protecting) sensitive sources and methods of information collected, through indices of information holdings, to "pointers" to inform one individual of another's precise or similar subject/target interest so that contact can be established and sharing or collaboration negotiated.

Finally, a widely understood, unwritten rule is the expectation in law enforcement that data access and sharing hinge on equitable participation. The so-called "pay-to-play" or "give-to-get" principle governs the meaningful sharing of information recommended in the methods and formal recommendations described in this Plan.

This portion of the *National Criminal Intelligence Sharing Plan* makes recommendations regarding information technology (IT) connectivity and systems compatibility to advance information and intelligence sharing. In so doing, the GIWG recognizes and promotes as the **highest** priority those systems that seek and provide full access to sensitive but unclassified information and intelligence by combining agencies' and organizations' investigative and intelligence data for common access through data warehousing and outreach or factual data search and retrieval and for data visualization though the application of analytical tools.

Data Warehouse

Data warehouse examples include, but are not limited to:

- The Multistate Anti-Terrorism Information Exchange™ (MATRIX) Program is a pilot effort that will initially connect participating states' criminal indices and investigative file databases, driver's license and motor vehicle registration databases, and other public records information for combined data query and sharing among law enforcement participants on the sensitive but unclassified RISS secure intranet (RISSNET™).
- The Gateway Information Sharing Initiative demonstration project in the St. Louis, Missouri, FBI field division, wherein some local, state, and federal criminal indices and investigative files are combined in a data warehouse and made available to all participating agencies for sophisticated factual search and retrieval and data visualization (link analysis and geo-mapping). Also included in the project is a classified data warehouse that adds classified FBI counterterrorism investigative data to the sensitive but unclassified holdings for exploitation by interagency members of the JTTF in the FBI field division.

These programs would each benefit from greater participation by additional local, state, and federal law enforcement agencies. Given the unique nature of these new endeavors, they should collaborate on developing factual data search and retrieval and data visualization tools, as well as shared experiences on crafting the governance arrangements and

associated participation memoranda of understanding.

Data Mart

Many law enforcement agencies may be prohibited by law or policy from participating in a data warehouse commingling of investigative data. To address these concerns, the GIWG proposes a data sharing method of the next highest priority: the so-called "data mart" approach, wherein the investigative indices, case files, and intelligence data are redacted, with the most sensitive case types (e.g., public corruption and internal conduct-related investigations) and the most sensitive data elements (e.g., informant identities) excised. The balance of the data is duplicated and presented in a separate database (data mart/information space) outside the agency's central database(s). Access can be by a variety of means, including a sensitive but unclassified connectivity, as presented later in this Plan.

"Pointer" Systems

Finally, the GIWG appreciates that some law enforcement organizations may not yet be familiar and comfortable with the breadth and depth of data warehouse-based or data mart sharing advocated above. With that recognition, law enforcement agencies are encouraged to mandate participation in "pointer" systems, wherein agents and investigators register investigative interest in a particular subject/suspect/target so as to ascertain which other law enforcement agencies and investigators (or officers within the same agency) might have a common investigative interest, might share information, or might consider participating in a joint investigation. Noteworthy ongoing databases for this purpose include, but are not limited to:

- The RISSIntel/RISSNET II databases, operated by the RISS centers.
- The U.S. Drug Enforcement Administration (DEA) National Drug Pointer Index (NDPIX).
- Certain High Intensity Drug Trafficking Area (HIDTA) case deconfliction/management databases.

Each of these databases operates in essentially the same manner. As a result of a law enforcement officer/agent registering investigative interest in a particular individual, the systems provide "pointers" identifying contact information to those with the same investigative interest. All receive the pointer information simultaneously and are notified that shared interests exist, whom to contact, and how to do so. Subsequent information sharing is a matter for mutual agreement, which is almost impossible without the pointer database capability.

The GIWG recognizes and recommends information sharing supported by collaborative communications networks and systems—joined together as a virtual single communications capability—as a means to overcome geographical distances, better support communications and investigative operational security, provide an audit trail of information shared, and ensure information access and transfer. Due to the use of identical technology mechanisms, the RISS and LEO interconnection offers a technically straightforward step in providing an initial nationwide sensitive but unclassified backbone for law enforcement connectivity. It is anticipated that this initial nationwide sensitive but unclassified communications capability will expand and evolve with the connection of other existing sensitive but unclassified enterprises, networks, and systems.

Refer to Recommendations 20, 21, 22, 23, 24, 25, 26, 27, and 28 for details and further discussion regarding this issue.

Recommendations for Implementation of the 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.

Discussion: 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 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.**

Discussion: The CICC should be structured similarly to the Counterdrug Intelligence Coordinating Group—a mechanism developed to provide management and oversight to the federal entities charged with implementing the *General Counterdrug Intelligence Plan of the National Drug Control Strategy*. Rules should be established that stipulate rotation of the chair between local, state, and federal representatives. Additionally, funding for the CICC should continue through OJP. It is recommended that the CICC be responsible for the following functions:

- Lead an effort to identify a framework for implementing and ensuring the longevity of the standards-based intelligence plan.
- Act as the governing body for the recommended communications capability.
- Represent all user groups and serve as an advisory council to the U.S. Attorney General, U.S. Department of Homeland Security (DHS) Secretary, and state governors.
- Perform a review of new systems/initiatives requesting connection to the communications capability, in order to determine adherence to guidelines/standards reference security, connections, data elements, and user backgrounds.
- Review proposed systems/initiatives to avoid duplicity with other established systems.
- Assist localities, states, and tribes in eliminating barriers in their laws and policies that limit intelligence sharing.
- Ensure coordination among departments and agencies responsible for systems participating in the nationwide communications capability.
- Submit an annual written report on the Council's activities to the U.S. Attorney General, national law enforcement organizations, and appropriate congressional committees.
- Monitor implementation of the *National Criminal Intelligence Sharing Plan*; the Council will adjust and modify the Plan as needed and required.

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 OJP beginning December 31, 2004, and annually thereafter.**

Discussion: Assessment of the various components of the Plan should occur at different phases of its implementation in order to measure the success of the project. Areas to evaluate should include community knowledge, training efforts, agency adoption of policies and standards, and systems participating in the nationwide communications capability. A time-interval series of surveys may be utilized and should be appropriately developed to various law enforcement levels (beginning with the implementation of the Plan, through use and benefits of the Plan). Consideration should also be given to developing performance measures to gauge the results and outcomes of the Plan.

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.**

Discussion: The Plan's action agenda cannot be meaningfully advanced with the existing resources of the nation's law enforcement community. This Plan will foster intelligence-led policing and strengthen homeland security, but simply stated, more local, state, and federal funding is critical to accomplish these goals. Without adequate funding, many of the recommendations, including improved training and technical infrastructure, will not be implemented, and the

country will remain at risk.

To date, the cost estimates for all of these initiatives have not been fully calculated. The CICC, in conjunction with law enforcement elements of the federal government and representative organizations of local, state, and tribal law enforcement, should calculate these resource requirements for presentation to the U.S. Attorney General, as the nation's chief law enforcement officer. Working with the Cabinet secretaries who have criminal law enforcement and homeland security responsibilities, the estimates should be included in the resource estimates presented as a cohesive funding strategy, with a special appropriations request analysis, to the Administration and the Congress for fiscal year 2005 appropriations.

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*. The National Signing Event should be held before December 31, 2003.

Discussion: Participants in the National Signing Event should include a wide range of law enforcement representatives from every level of government and major law enforcement organizations. Conducting outreach and marketing efforts regarding the Plan is imperative prior to the National Signing Event. Those agencies signing on to the Plan should have a clear understanding of what the commitment entails.

The education process should include national law enforcement organizations, such as the IACP, the Fraternal Order of Police, and the NSA; local and state law enforcement associations/ organizations; and entities of local, state, tribal, and federal law enforcement. Specific groups should be targeted for presentations regarding the Plan at national conferences.

Additionally, press conferences should be held to promote public acceptance of the Plan. One of the most important aspects of information sharing in the law enforcement and intelligence domains today is ensuring public trust and awareness. Each step of the process must include education and outreach to the communities served. The public must be constantly aware of what type of information is used to enhance public safety and how it is processed. Outreach, education, and public awareness are crucial for success and must be considered from the outset.

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.

Discussion: In this post-9/11 era, the need for criminal intelligence sharing is more compelling than ever. The public's demand that law enforcement agencies do all they can to prevent terrorism—including the effective sharing of criminal intelligence—is also clear. Legislatures and individual elected officials, likewise, demand that agencies share criminal intelligence so that overall patterns of criminal activity, undetectable within a single jurisdiction, can be observed when the whole is examined. Rapid technological advances offer the promise of making criminal intelligence sharing even more efficient, effective, timely, and secure. What, then, could stop this momentum towards criminal intelligence sharing?

One of the critical issues that could quickly stop intelligence sharing is the real or perceived violation by intelligence sharing systems of individuals' privacy and constitutional rights. To understand why, one must consider the context in which the sharing of sensitive and often preliminary criminal intelligence information operates.

First, both constitutional values and an individual's right to privacy are deeply embedded in our nation's laws, culture, and expectations. Our nation's preference for government restraint has a long and conspicuous history in America. Our founding fathers, fearful of a large, centralized, and authoritarian government, crafted the Bill of Rights to limit the power of government. These guarantees include freedom of thought, belief, expression, and assembly; protection against unreasonable searches and seizures; and provisions for a court hearing prior to the government's taking of a person's life, liberty, or property. Similarly, although there is no explicit federal constitutional right to an individual's privacy,[26] privacy rights have been articulated in limited contexts by the U.S. Supreme Court.[27] In fact, Justice Louis Brandeis observed that the "right to be left alone" is the most comprehensive of rights and the right most valued by a free people.[28] Individuals' information privacy interests have also been articulated in federal and state case law and protected in statutes and regulations governing collection, use, and sharing of justice information, including criminal intelligence systems (see, for example, 28 CFR Part 23). Thus, the American tradition includes a healthy suspicion of unrestrained government and a fervent demand by the public that their government does

26 U.S. Constitution Amendment IV. See California Constitution article 1, §1 (West 1983).

27 National Criminal Justice Association. 2002 (September). *Justice Information Privacy Guideline: Developing, Drafting and Assessing Privacy Policy for Justice Information Systems*. Washington, DC: NCJA, p. 18-19.

28 Olmstead v. U.S. (1928).

not infringe on the constitutional rights of the people nor unnecessarily violate an individual's privacy.

Second, the public perception of current intelligence work is strongly shaped by its recent history. Since the 1960s, overzealousness by some criminal intelligence units has periodically led to infringements on civil liberties. For example, some individuals have been targeted for surveillance and other investigative activities apparently based solely on their constitutionally protected exercise of free speech, expression of political beliefs, and other lawful activities. These law enforcement actions involving the misapplication of the criminal intelligence function have resulted in lawsuits and judgments against some of the agencies involved.[29] In fact, some law enforcement agencies completely disbanded their criminal intelligence units[30] in the face of allegations of abuse. This history directly affects how the public perceives intelligence work and how it judges the effectiveness of any proposed policy that addresses the protection of constitutional rights and individuals' privacy. It also demonstrates how the continued existence and operation of the criminal intelligence function in a law enforcement agency may be affected by improper criminal intelligence practices.

The protection of individuals' privacy and constitutional rights is, therefore, an obligation of government officials and is crucial to the long-term existence and success of criminal intelligence sharing. Consequently, it is important to advocate policies and practices that accomplish this goal. Indeed, the *National Criminal Intelligence Sharing Plan* will provide model criminal intelligence policies for law enforcement agencies to use that will protect the privacy and constitutional rights of individuals. However, it must be recognized that policies are merely a means to an end—the protection of individual rights within the intelligence process. Achieving that end, 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. This commitment, however sincerely held, will not have the necessary intensity or staying power unless it becomes part of the culture of the criminal intelligence community. This goal will require the sustained effort and focus of all participants in the implementation and operation of the *National Criminal Intelligence Sharing Plan*.

It is important that the commitment to protect individuals' privacy and constitutional rights is prominently highlighted in all areas of the Plan. Outreach activities should be proactive on this mandate, both within the law enforcement community and with the general public. Law enforcement officials must be assured that protecting the privacy and constitutional rights of individuals will not hinder the effectiveness of their agency's 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.**

Discussion: All elements of our society have a stake in protecting and reducing the United States' vulnerability to terrorist attacks. Currently, the private sector controls 85 percent of America's critical infrastructure. Critical infrastructure is defined as those systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Protecting America's critical infrastructures requires cooperation among all levels of government and the private and public sectors. DHS is the lead agency responsible for evaluating vulnerabilities; issuing warnings and advisories; and coordinating with other local, state, tribal, and federal agencies and private entities to ensure the most effective homeland security response for America's public safety agencies, elected officials, industry, and the public. Information sharing is vital to the homeland security effort; law enforcement and public safety agencies must use the capabilities of the private sector to achieve a practical level of security without hindering productivity, trade, or economic growth. Cooperative efforts, such as the critical infrastructure pilot project initiated by DHS, should continue and expand as mechanisms for the receipt and exchange of important information are developed and fine-tuned.

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.**

Discussion: An Outreach Package has been prepared to publicize and promote the concepts and standards contained within the *National Criminal Intelligence Sharing Plan*. Samples of materials prepared include an article, brochure,

29 American Friends Service Committee. 1979. *The Police Threat to Political Liberty*. Philadelphia, PA: American Friends Service Committee.

30 Martens, Frederick T. 2000. "Uses, Abuses, and Misuses of Intelligence." In Marilyn B. Peterson (Managing Ed.), Bob Morehouse, and Richard Wright (Eds.), *Intelligence 2000: Revising the Basic Elements*, Sacramento, CA: Law Enforcement Intelligence Unit, and Lawrenceville, NJ: International Association of Law Enforcement Intelligence Analysts, Inc., pp. 37-47.

and a CD containing testimonials from several law enforcement officers and an explanation of the Plan.

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 28 CFR Part 23,[31] regardless of whether or not an intelligence system is federally funded.

Discussion: Federal regulation 28 CFR Part 23 is a guideline for law enforcement agencies that contains implementing standards for operating federal grant-funded, multijurisdictional criminal intelligence systems. It specifically provides guidance in five primary areas: submission and entry of criminal intelligence information, security, inquiry, dissemination, and the review-and-purge process. The 28 CFR Part 23 regulation does not provide specific, detailed information on how the standards should be implemented by the operating agency, but it provides for each agency to develop its own policies and procedures. This regulation is currently pending revision. The proposed revisions are the result of three major concerns: the speed at which technology changes, the nature of the new threat to public safety (exemplified by terrorism), and the critical need to facilitate information sharing among all levels of government.

Recommendation 10: Law enforcement agencies should use the IACP's *Criminal Intelligence Model Policy* (2003 revision)[32] as a guide when implementing or reviewing the intelligence function in their organizations.

Discussion: In 1987, the IACP entered into a cooperative agreement with the Bureau of Justice Assistance (BJA), DOJ, to establish a National Law Enforcement Policy Center ("Center"). The objective of the Center was to assist law enforcement agencies across the country in the critical and difficult task of developing and refining law enforcement policy. Organized under the direction of a broad-based advisory board of recognized law enforcement professionals, the Center has carried out its mission through the development of a wide variety of model law enforcement policies. Each model incorporates the research findings, the input of leading subject-matter experts, and the professional judgment of advisory board members who have combined this information with their extensive practical field and management experience.

The *Criminal Intelligence Model Policy* was originally promulgated in February 1998. The purpose of the 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 Center, suggested revisions to the *Criminal Intelligence Model Policy*. The revised Policy was presented to the Center Review Board in June 2003 and was approved at that time.

Recommendation 11: In addition to federal regulation 28 CFR Part 23, law enforcement agencies should use the LEIU *Criminal Intelligence File Guidelines* as a model for intelligence file maintenance.[33]

Discussion: The LEIU, in existence since 1956, is a network of intelligence specialists from nonfederal law enforcement agencies nationwide that promotes the gathering, recording, and exchange of criminal intelligence. The LEIU first developed the *Criminal Intelligence File Guidelines* in the 1970s to promote professionalism, provide protection of citizens' privacy, and provide guidance to their member law enforcement agencies when collecting information in the pursuit of preventing and solving crimes. Law enforcement agencies involved with intelligence gathering should operate under specific guidelines in order to ensure that abuses do not occur. It is recommended that agencies also adopt file procedures as a check and balance against inappropriate activities. The LEIU *Criminal Intelligence File Guidelines* can provide law enforcement agencies with a foundation for establishing sound standards regarding maintenance of their criminal intelligence files.[34]

Recommendation 12: The 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). These minimum standards should be developed by June 30, 2004. Law enforcement agencies should adopt these standards as soon as developed and approved by the CICC.

Discussion: The role of analysis in a law enforcement agency is to support the investigative, planning, and intelligence activities of the agency. Thus, the work that is performed by

31 The 28 CFR Part 23 regulation is included on the companion CD and is also available at www.iir.com/28cfr/guideline1.htm.

32 The IACP *Criminal Intelligence Model Policy* is included on the companion CD and is also available at www.theiacp.org.

33 The March 2002 update of the LEIU *Criminal Intelligence File Guidelines* is included on the companion CD.

34 Civil liberties groups, citizens, and government and police officials have agreed that the standards embodied by LEIU are proper for collecting, maintaining, and disseminating criminal intelligence information. See the "Settlement Agreement and Release" entered into by and between Joseph N. Riggs III, Alice Hector, Peter Cubra, James R. Toulouse, Tova Indritz, Randi McGinn, Nancy Hollander, Sigmund Bloom, Hank Farrah, Joe Fine, Dorie Bunting, Allen Cooper, Richard Moore, The American Civil Liberties Union of New Mexico, and The New Mexico Chapter of the National Lawyers Guild, and the City of Albuquerque, dated September 29, 1993, resolving Cause No. Civ. No 88-1141 JP/RWM in the United States District Court for the District of New Mexico, and CV-91-07599, Second Judicial District Court, County of Bernalillo, State of New Mexico.

an intelligence function should reflect the priorities and goals of the specific agency or organization. There is a range of analytic products that result from a careful and thorough review of varied documents, and the types and formats of intelligence products also vary (e.g., working reports, analytic reports, assessments, or reports of raw data). Regardless of the format, intelligence products must be accurate, timely, and factual. "Reports are the very lifeblood of the intelligence process," and "intelligence reporting is the basis most often used for judging the value of a police intelligence unit."[35] Therefore, it is critical that reports be done and that they be done well.

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.**

Discussion: Participation in professional criminal intelligence organizations in conjunction with comprehensive, high-quality training offers promise for ensuring that working group norms in law enforcement agencies foster the protection of individuals' privacy and constitutional rights. Active participation in professional organizations encourages professional development, including a commitment to ethical service, continuous learning about the profession, peer evaluation, and openness and accountability to all stakeholders. Participation in professional organizations also develops trust and confidence among members, as well as from the justice and public safety communities. All of these features are particularly salient to the important issue of protecting individuals' rights. In addition to encouraging participation in professional criminal intelligence organizations, the *National Criminal Intelligence Sharing Plan* must also encourage appropriate training to be widely available on this topic. Through the use of core training curricula, all levels of law enforcement should be educated on constitutional rights, privacy issues, and safeguards as they relate to the criminal intelligence function.

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.**

Discussion: The police consistently rank high among the institutions and occupations in which the public expresses confidence and trust.[36] Although many indicators show that American police are among the most trusted and admired institutions of contemporary society, there are also many indicators that some citizens are wary of the police.[37] This may be especially true in the area of the criminal intelligence process.

At least two factors combine to make earning the public's trust in the intelligence process an especially important and key part of long-term, successful intelligence sharing. First, put simply, the public's trust in intelligence work has been reasonably shaken in the past through the disclosure of excesses and abuses. Second, by its very nature, criminal intelligence work is often unseen or unobserved by the public. These two factors can contribute to diminished trust in the application of the intelligence process and a lack of understanding in how it is carried out.

But that same public trust is necessary for successful criminal intelligence sharing. Trust gives law enforcement agencies greater access to valuable information that can lead to the prevention and solution of crimes. It also engenders support for law enforcement efforts.[38] Public cooperation and support can be obtained most readily if public trust and confidence exist in the intelligence process.

A general policy of openness can foster public trust in law enforcement agencies. A principle of openness about criminal intelligence processes should therefore be applied whenever possible. Of course, criminal intelligence information is confidential and must be protected from unauthorized disclosure, but the operating principles of the intelligence process can be open and accessible to the public. This approach can demystify the intelligence process and defuse suspicion that might be generated by the sometimes shrouded and enigmatic nature of the criminal intelligence 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*,[39] which law enforcement agencies should**

35 Parks, Dean and Marilyn Peterson. 2000. "Intelligence Reports." In Marilyn B. Peterson (Managing Ed.), Bob Morehouse, and Richard Wright (Eds.), *Intelligence 2000: Revising the Basic Elements*, Sacramento, CA: Law Enforcement Intelligence Unit, and Lawrenceville, NJ: International Association of Law Enforcement Intelligence Analysts, Inc., pp. 121-133.

36 Source: Harris Interactive, Inc., *The Harris Poll*, Feb. 7, 2001, pp. 4-6; Jan. 30, 2002, pp. 3, 4 (Los Angeles: Creators Syndicate, Inc.). Cited in Ann L. Pastore, and Kathleen Maguire (Eds.), Sourcebook of Criminal Justice Statistics [Online]. Available: http://www.albany.edu/sourcebook/, May 3, 2003, at Table 2.13.

37 Gallagher, Catherine, Edward R. Maguire, Stephen D. Mastrofski, and Michael D. Reisig. 2001 (October 2). *The Public Image of the Police: Final Report to The International Association of Chiefs of Police by the Administration of Justice Program*, George Mason University. Accessed on the World Wide Web at http://www.theiacp.org/profassist/ethics/public_image.htm, May 3, 2003.

38 From the Web site of the Community Policing Consortium, http://www.communitypolicing.org/about2.html, May 3, 2003.

39 This document is included on the companion CD and is also available at http://www.ncja.org/pdf/privacyguideline.pdf.

employ to ensure protection of individuals' privacy and constitutional rights and to identify and remedy practices that are inconsistent with policy.

Discussion: Accountability is essential to the effective implementation of a policy designed to protect individuals' privacy and constitutional rights. It acknowledges a responsibility to ensure that the standards specified in the policy are carried out in the field. Frequently, a gap occurs between a policy and the actual practices that occur in "real life." Accountability mechanisms reduce that gap, which, in turn, reduces liability to the agency. Accountability mechanisms are the invisible bridge from words on paper (i.e., the policy) to actions in the field.

The primary responsibility for ensuring accountability rests with law enforcement agencies themselves.[40] Policing expert Herman Goldstein has argued, "The nature of the police function is such that primary dependence for the control of police conduct must continue to be placed upon internal systems of control." Most police experts assert that internal mechanisms of accountability are more likely than others to be effective for at least two reasons: (1) department officials have direct, day-to-day contact with the work that is conducted and thus are "closer" to the situation, and (2) officers are more likely to understand and respect rules that are developed by law enforcement agencies.[41] By the same token, agencies must take seriously the need for effective implementation of accountability measures.

The *National Criminal Intelligence Sharing Plan* identifies a wide array of suggested accountability mechanisms, such as periodic review 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.[42]

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*.[43] The goal of the *Justice Information Privacy Guideline* (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.**

Discussion: Some privacy issues can be addressed through following basic tenets of information collection and use; the *Justice Information Privacy Guideline* provides specific direction on how to employ good collection and use practices. The Guideline also discusses a number of other privacy issues that are not as easily resolved, such as determining the sensitivity or public accessibility of certain data. The Guideline is the result of a two-year collaboration of local, state, and tribal justice leaders, as well as academia, elected officials, media, and the private sector. The GAC, through its Global Privacy and Information Quality Working Group, coordinated production of the Guideline.

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. The technical means for production of these reports should be identified by June 30, 2004.**

Discussion: The law enforcement and intelligence communities routinely protect the sources of information and the methods by which that information is garnered. In this manner, the identities of confidential police sources are routinely excised from reports. For classified information, the procedure is unchanged, but more difficult. The data in its entirety is classified, although the basis for the classification relates to the source or the technical means by which the information was acquired. The Plan does not recommend any change to those rules and classification procedures.

To that end, two approaches are recommended:

1. Use "reports" officers/analysts to generate and disseminate sanitized reports of current law enforcement investigative information to their counterpart law enforcement agencies at the local, state, tribal, and federal levels. Establishing such a capability can markedly and actively enhance law enforcement information sharing. Doing so necessitates the dedication of a cadre of intelligence analysts in the federal law enforcement agencies, especially the U.S. Drug Enforcement Administration (DEA), FBI, and U.S. Customs

40 Goldstein, Herman. 1977. "Controlling and Reviewing Police-Citizen Contacts," in *Policing a Free Society*. Cambridge, MA: Ballinger, pp. 157-186.

41 Walker, Samuel. 1999. *The Police in America*, Third Edition. Boston, MA: McGraw-Hill College, p. 279, citing Goldstein, Herman. 1967. "Administrative Problems in Controlling the Exercise of Police Authority." *Journal of Criminal Law, Criminology and Police Science,* 58, pp. 160-172.

42 Audits of this type have been successfully conducted by the Executive Board of the Law Enforcement Intelligence Unit (LEIU) for some law enforcement agencies.

43 This document is available at http://www.ncja.org/pdf/privacyguideline.pdf.

and Border Protection headquarters and field offices. Their primary mission is to ensure that timely and high-value, but not case-sensitive, information is provided to those with a need to know—while protecting sensitive, undercover, and legally restricted law enforcement sources, information, individuals, and techniques. The law enforcement community needs a reporting capability comparable to the intelligence community's reports officer to push out valuable information from law enforcement field offices to their own headquarters elements.

2. Establish procedures and designate supervisors to pass and receive sensitive "tips and leads." Information sharing, as currently practiced, includes the use of tips and leads to trusted individuals who may direct subordinate agents/officers to take actions without informing them of the basis for that action. As such, designated supervisors serve as a "cut-out"; they can appreciate the value of shared information yet not reveal the source of shared information to subordinates. Law enforcement investigations may be thus initiated, directed, or developed from the facts observed, without including the intelligence that prompted the agents/officers to be in a position to make those observations.

Attempts to tag data in its initial preparation, so as to identify the sensitive sources and methods, are ongoing; however, a philosophical change by the agencies that prepare classified documents may be required in order to fully implement this process. Reports should be prepared in such a manner that all content below a certain line in the document or message is of a lower classification. This method protects sensitive sources and methods of higher classification and provides a discernable marking in the document or message where information may be shared.

Evidence of the ongoing efforts to provide classified data to local law enforcement includes a bill, currently pending before Congress, that would authorize the DHS to conduct a pilot project in which intelligence information from DHS is made available to officials of local and state governments through the use of tear-line intelligence reports. Efforts to automate these redactions (e.g., interface filters) are encouraged, so as to ease the preparation of declassified reports and tear-line reports of classified data.

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.[44]

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.

Discussion: The IACP *Criminal Intelligence Sharing Report* identified several recommendations specific to training issues:

- Training should provide recipients with the skills to provide more targeted, evaluative summary data to decision makers.
- Appropriate training must be provided to in-service law enforcement personnel and basic recruits on information sharing systems and criminal intelligence concepts.
- Training should promote building trust for intelligence sharing.
- Training should promote protection of civil and constitutional rights.
- Training should emphasize that all personnel, regardless of position, have a role in the intelligence process and information sharing.
- Training should equip personnel to use new technologies.

It is important that recognition be given to those individuals and agencies that participate in the training curriculum. Certificates of Completion should be given to each individual who participates in the varied levels of intelligence training by the entity delivering the training.[45]

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

Discussion: IADLEST is an international organization of training managers and executives dedicated to the improvement of public safety personnel. Every state is represented in its membership. The mission of IADLEST is to research, develop, and share information, ideas, and innovations that assist states in establishing effective and defensible standards for employment and training of peace officers. Additionally, IADLEST recommends model minimum state standards in the following areas: entry-level standards, basic training, in-service requirements, discipline and decertification, and curriculum issues for criminal justice officers. As a national association of training managers, IADLEST can effectively liaison with local, state, tribal, and

44 The recommended training standards for each level, including roles and missions, core training objectives, and length of training, are included in the appendix of this report and on the companion CD.

45 A wide range of training is available from local, state, regional, and federal providers. A listing of available intelligence training sources and specifically scheduled classes may be found at www.ialeia.org. This listing is updated on a semiannual basis and also allows individuals to directly contact training source agencies and organizations for more information on classes and schedules.

federal training academies and other training providers to make curriculum changes in support of new intelligence sharing goals. The membership of SPPADS, which was established by IACP to advance the principles and competency of professional law enforcement instructors, should also be utilized to effect changes in curriculum at the local and state levels.

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.**

Discussion: For more than 75 years, the FBI's Uniform Crime Reporting (UCR) Program, with more than 16,000 law enforcement agencies contributing crime statistics, has served as the principal means to measure crime in America. To move this important program into the twenty-first century, the FBI partnered with other local, state, and federal agencies to create a new, automated National Indices and Pointer System that will be designed to collect data on each crime occurrence and arrest associated with that occurrence.

The most significant difference between incident-based reporting and the traditional UCR system is the timeliness and degree of detail in reporting. Unlike the traditional or "summary" UCR system, which collects statistics on only a handful of major crimes (often after several months of reported lag time), the incident-based reporting system collects data on approximately 50 criminal offenses in near real-time, drawing the data from the day-to-day internal records management systems used by participating law enforcement components. The goals are to enhance the quantity, quality, and timeliness of crime data collection by law enforcement so as to improve the methodology used for compiling, analyzing, auditing, and publishing the collected criminal statistical data.

Today, some 4,200 law enforcement components throughout the country employ internal, Web-based, incident-based records management systems for internal records storing that are compatible with the National Indices and Pointer System. Much more is needed to make this useful initiative a core element of criminal intelligence sharing. These participating 4,200 components represent jurisdictions that cover only 17 percent of the nation's population. The FBI's Criminal Justice Information Services (CJIS) Division encourages and assists additional jurisdictions to deploy information systems to achieve incident-based reporting.

The CJIS Division envisions a System of Services Information Sharing System that capitalizes upon and integrates its IT systems housed at the CJIS Division—the UCR System; the Integrated Automated Fingerprint Identification System (IAFIS); the National Crime Information Center (NCIC); the Interstate Identification Index or criminal history records; the denied persons file of the National Instant Criminal Background Check System (NICS); its aggregation of local, state, and federal incident-based law enforcement data reporting; CJIS-supported telecommunications systems; and the FBI Law Enforcement Online (LEO) system, which is linked to RISSNET. The FBI's vision is to provide a consolidated report of all criminal information relative to an individual's contacts with law enforcement.

The Chicago Citizen and Law Enforcement Analysis and Reporting (CLEAR) system exemplifies the intelligence value of such a local, statewide, regional, or metropolitan system to the deploying agency. CLEAR's coverage includes the 132 police jurisdictions in Cook County, Illinois (including field components of the Bureau of Alcohol, Tobacco, Firearms and Explosives; the FBI; and the U.S. Marshals Service), as well as future plans to incorporate the Illinois State Police LEADS system (Law Enforcement Agency Data System consisting of 1,200 law enforcement data systems of the other jurisdictions in the state of Illinois). CLEAR provides a repeatable, integrated criminal justice records system. It presents real-time, relational information of value to operations, policymakers, and participating police agencies. Presently, the Chicago Police Department and the Illinois State Police are piloting wireless access to CLEAR statewide. CLEAR's database serves 25,000 law enforcement officials with the following capabilities: holds information and digital photos on 7 million offenders and 3 million incidents, compares and links any database elements, records information on all law enforcement stops, provides warnings relative to want notices, and conducts link and pattern analysis. CLEAR is credited with permitting the redeployment of 90 officers to enforcement activities, the elimination of 330 clerical positions, a 20 percent improvement in officer effectiveness, and savings in excess of $15 million.

The value of an incident-based records system is important first to the implementing jurisdictions and its citizens. The value of such a system (and the information that could be derived from it) is also important to a national statistical system, such as the envisioned FBI System of Services. With better UCR data, law enforcement stands to better track criminal trends for policymakers and the Congress; with

incident-based data, the integrated databases of the FBI CJIS Division can provide valuable criminal information and potential intelligence across jurisdictions at a level of granularity that can assist in crime prevention and crime solving. In this regard, the CLEAR program is currently engaged in planning to provide incident-based data needed by the FBI incident-based records system, though at present only summarized UCR statistics are provided.

Recommendation 21: **RISS and the FBI 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.**

Discussion: 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 single system for local, state, tribal, and federal law enforcement, intelligence community agencies, the diplomatic community, and first responder connectivity. Six sensitive but unclassified systems and networks have been identified[46] with national coverage. Other sensitive but unclassified systems and networks exist with admirable and similar capabilities (with significant information sharing capabilities and security) but with local, state, or regional geographical coverage.[47] The first four sensitive but unclassified systems and networks listed in footnote 46 apply primarily to law enforcement agencies and have considerable capacities, capabilities, and scope; yet, taken individually, they remain relatively limited in use in terms of intelligence sharing by the aggregate of local, state, tribal, and federal law enforcement agencies and personnel.

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. The capabilities identified above—and their collective membership of some 150,000 current users—should be built upon; connected to one another and to other sensitive but unclassified communications capabilities; and expanded, not replicated or kept static.

Consequently, the consensus of law enforcement representatives to the GIWG recommends leveraging, strengthening, and expanding existing systems by adding users and connecting local, state, and regional systems. In essence, this means maximizing existing systems by connecting them to expand collaboration opportunities and database access, while continuing to evolve the nationwide sensitive but unclassified architecture to support fully functional, bidirectional information sharing. The recommended "system of systems" network is trusted, secure, and accessible by all levels of law enforcement. It should, and can, support collaboration with homeland security officials and the first responder community. It must have greater capacity to handle the larger volume of information transactions. As the first crucial step in response to the need for greater information sharing among local, state, tribal, and federal law enforcement, OJP provided funding for the interconnection of the RISS and LEO systems. This was achieved in September 2002.

The RISS and LEO interconnection is recommended as the initial nationwide connectivity backbone for several reasons. The RISS Program is a secure nationwide communications and information sharing network that serves over 7,000 law enforcement member agencies from all government levels, with members in 50 states, the District of Columbia, U.S. territories, Canada, Australia, and England. Internet technology and virtual private network (VPN) software provide an encrypted, secure intranet that is able to connect member agencies to the databases of six regional RISS centers and five other intelligence systems from a single query via RISSNET. In essence, while six RISS regions exist, there is but one RISSNET. Additionally, several High Intensity Drug Trafficking Areas (HIDTAs), state intelligence systems, the LEIU network, and the nationwide Clandestine Laboratory Seizure System are accessible via RISSNET.

46 The six sensitive but unclassified systems identified are as follows: 1) Regional Information Sharing Systems' secure intranet (RISSNET), funded by the U.S. Department of Justice (DOJ), Office of Justice Programs, and membership fees of participating local and state law enforcement departments and agencies and also some federal law enforcement agencies' field divisions and field offices; 2) Law Enforcement Online (LEO), funded by DOJ; 3) the International Justice and Public Safety Information Sharing Network (NLETS); 4) Anti-Drug Network-Unclassified (ADNET-U), provided to law enforcement agencies primarily along the Southwest Border by the U.S. Department of Defense (DoD), Defense Information Systems Agency (DISA); 5) Open Source Information System (OSIS), provided to the intelligence community, military, law enforcement, and diplomatic community agencies by the Intelligence Community Chief Information Officer through the Intelink Program Management Office; 6) OpenNet Plus, provided by the U.S. Department of State (DOS) to the 40-plus U.S. government agencies' representatives at 250 embassy sites internationally and the DOS headquarters.

47 Examples include, but are not limited to the following: a) the Automated Regional Justice Information System (ARJIS)—a complex criminal justice enterprise network utilized by 38 local, state, and federal agencies in the San Diego, California, region. The ARJISNet secure intranet contains data on the region's crime cases, arrests, citations, field interviews, traffic accidents, fraudulent documents, photographs, gang information, and stolen property, and b) CriMNet—an enterprise architecture that puts in place a statewide framework of people, processes, data, standards, and technology focused on providing accurate and comprehensive data to the criminal justice community in the state of Minnesota.

To date, RISS has some 60,000 "access officers" approved to receive information and services from RISS for 7,000 law enforcement agencies, representing some 700,000 officers. Approximately 18,000 users have active RISSNET accounts, including some 1,000 federal law enforcement agents and analysts. RISS needs additional funding to add some 6,000 local, state, and tribal member agencies, adding approximately 20,000 "access officers," so that 80 percent of local, state, and tribal law enforcement personnel nationwide are represented and have access to those who, in essence, have intelligence information that warrants sharing and the staff to react to that information.

The FBI-hosted LEO system is a nationwide source of law enforcement intelligence that is compiled from many sources, can be subscribed to by Internet-enabled law enforcement personnel, and is funded by DOJ. It functions as an information repository but also features segmented community-of-interest areas with multilevel controlled access for specialized law enforcement groups that have their own members (termed LEO Special-Interest Groups, or SIGs), interactive chat groups, electronic calendars, listserv intelligence "push" capability, and secure e-mail options—all of which additionally support intelligence exchange.

To date, LEO has some 25,000 users, of which approximately two-thirds are local, state, and tribal law enforcement personnel. On September 19, 2002, the FBI Executive Assistant Director for Law Enforcement Services invited federal law enforcement agencies to identify an initial 5,000 new law enforcement personnel to be added to LEO with FY2002 resources.

The FBI has proposed expanding LEO to local, state, tribal, and federal law enforcement personnel and has plans to rely on it for sensitive but unclassified communications for emerging FBI data systems.

The FBI has selected and tested a National Alert System (NAS) for another 21,000 law enforcement personnel on LEO. Unique from the current homeland security bulletins now transmitted via LEO, RISSNET, and the International Justice and Public Safety Information Sharing Network (NLETS), it has the capability to interrupt an ongoing LEO session with sounds and eye-catching visuals to call attention to the alert message. The system can cast its alert broadly, as it presently occurs, or more narrowly to pertinent recipients. The alert links LEO recipients to more detailed information at secure, encrypted sites. Further, the system is not Internet-dependent. A message notifying that an alert has been sent is also transmitted to secondary and tertiary devices, such as pagers, telephones, and cell phones, as stipulated by the individual LEO recipient. The individual LEO recipient can also include such devices for ten additional law enforcement colleagues. The FBI contemplates implementation of the NAS in the near future.

The nationwide RISS and LEO interconnection employs full encryption. Technologically, a VPN is initiated from current desktop and stand-alone Internet connections to achieve secure, encrypted connection and single sign-on access privileges to the connected systems. Privileges granted separately to members of each system can be exercised at the same time whether through LEO or RISS; access privileges granted to RISS members can be exercised through the LEO connectivity with RISS; access privileges granted by LEO can be accessed through the RISS connectivity with LEO. The cost for use of these systems is minimal for RISS users and free for LEO users; the cost of the existing and proposed expanded sensitive but unclassified communications capability is markedly less than the creation of a new network or system. This cost-effective approach could be further amplified by leveraging infrastructure investments of other existing sensitive but unclassified enterprises through the implementation of industry standards-based interconnections.

In February 2002, the CDX, the interagency staff element of the Counterdrug Intelligence Coordination Group (CDICG), an interagency intelligence sharing body comprised of representatives of eight Cabinet principals and the five heads of federal law enforcement with drug law enforcement missions, proposed that "federal law enforcement agencies[48] endorse, select, and take steps to join the FBI LEO system as the primary sensitive but unclassified e-mail and collaboration environment for federal law enforcement agencies and for connectivity (through RISS) with local and state law enforcement." The U.S. Attorney General, the Deputy Attorney General, the FBI Director, the DOJ Chief Information Officer (CIO), and 13 federal law enforcement agencies endorsed this sensitive but unclassified connectivity.[49] The Homeland Security IT Investment Review Board of Agency CIOs and the DHS CIO also endorsed this connectivity plan.

Finally, the RISS and LEO systems are recommended as the initial communications backbone for the *National Criminal Intelligence Sharing Plan*, given that no other system has been identified that can provide local, state, tribal, and federal nationwide communication connectivity. In a recent House Appropriations Committee report regarding funding for RISS,

48 The term *federal law enforcement agencies*, as used herein, connotes federal agencies with criminal law enforcement authorities, particularly those involved in drug law enforcement activities, and also includes, but is not limited to, those involved in counterterrorism and homeland security activities. The definition here does not include the Offices of the Inspectors General.

49 The RISS/LEO interconnection for sensitive but unclassified information sharing is endorsed by the following: U.S. Drug Enforcement Administration; Federal Bureau of Investigation; U.S. Customs Service; Executive Office for United States Attorneys; Organized Crime Drug Enforcement Task Force Program, Criminal Division; U.S. Secret Service; U.S. Postal Inspection Service; U.S. Forest Service; U.S. Coast Guard; Bureau of Alcohol, Tobacco, Firearms and Explosives; Internal Revenue Service; U.S. Marshals Service; U.S. Department of Commerce, Bureau of Industry and Security; National Drug Intelligence Center; El Paso Intelligence Center; Financial Crimes Enforcement Network; Intelligence Community Chief Information Officer; Deputy Chief Information Officer, Community Management Group, Central Intelligence Agency; High Intensity Drug Trafficking Areas Program Office; Office of National Drug Control Policy; and Defense Information Systems Agency, U.S. Department of Defense.

the following was reported, "The Committee is pleased with the Administration's efforts to integrate RISS with the LEO program and with the proposed expansion of RISS Automated Trusted Information Exchange (ATIX) and the MATRIX Program. The Committee expects OJP to coordinate their efforts with other components of the U.S. Department of Justice and with the U.S. Department of Homeland Security to ensure that state and local agencies have electronic access to crime and terrorism information. The Committee remains concerned at the continuing proliferation of local, state, regional, and federal information sharing initiatives that are being developed independently, with no apparent plan to integrate them with other systems operated by federal law enforcement agencies and with RISS and LEO. The Committee directs the Department to ensure that interstate information sharing systems funded by OJP and the Office of Community Oriented Policing Services utilize the existing communications infrastructure and are compatible with RISS and LEO."[50]

Additional congressional recognition of RISS and LEO was cited in a recent Senate Appropriation Committee report. "The Committee commends the ongoing collaboration between RISS and LEO, particularly with regard to the decision to provide access to RISS ATIX™ resources to any user holding a valid LEO account, regardless of whether the user also holds a RISS account. The Committee recognizes that the relationship between RISS and LEO is dynamic and evolving, and strongly supports further collaboration."[51]

This recommendation proposes the utilization of the RISS/LEO sensitive but unclassified communications capability as providing a network that supports nationwide sensitive but unclassified communications. By definition, a communications backbone denotes the flow of communications bidirectionally. This Plan acknowledges the existence of and allows for other network connections within and between communities represented by agencies and programs but strongly encourages that a fully functional path between community sensitive but unclassified users and resources and the national sensitive but unclassified communications capability be provided. The phrase *fully functional* denotes supporting enterprise-to-enterprise, user-to-application, and user-to-user/system-to-user messaging capabilities and system resource access (databases, communities of interest, discussion groups, home pages, etc.) while maximizing the use of existing participant infrastructures; i.e., existing program/community authentication methods, governance and vetting processes, and networks. The intent is to have the nationwide sensitive but unclassified communications capability provide a highly flexible architecture and baseline policy to rapidly facilitate information sharing through the reuse of existing participant and program resources (hardware, software, and personnel).

The *National Criminal Intelligence Sharing Plan* promotes and encourages law enforcement agencies to join in the data access and collaboration capabilities enabled by the proposed nationwide sensitive but unclassified communications backbone.

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.[52]**

Discussion: The RISS/LEO interconnection is used for communicating investigative and intelligence data on all types of crimes. However, the need for the exchange of information extends beyond law enforcement and beyond RISS and LEO. Law enforcement agencies should expand sensitive but unclassified collaboration with the intelligence and diplomatic communities. Further, law enforcement agencies should, and can, communicate and share information and intelligence in a sensitive but unclassified environment with first responders, public safety, and others engaged in the broad homeland security mission.

To this end, the RISS/LEO interconnection is in the process of expanding with connections to the Intelligence Community Open Source Information System (OSIS), the U.S. Department of State (DOS) OpenNet Plus network, and the Defense Information Systems Agency (DISA) Anti-Drug Network-Unclassifed (ADNET-U) system. Connectivity expansion is in process with NLETS for both RISS and LEO and is being considered with the U.S. Department of Defense (DoD) Unclassified but Sensitive Internet Protocol Router Network (NIPRNET).

The FBI agreed with the Intelligence CIO and the Intelink Program Manager to connect their OSIS to the RISS/LEO interconnection; that connection is planned for September 2003. This will provide LEO and RISS users with access to OSIS commercial databases and OSIS users through encrypted sensitive but unclassified e-mail. Further, the Intelligence Community contemplates establishing an Information Manager resource on OSIS for law enforcement to make known its investigative interests to the Intelligence Community, to examine its agencies' classified holdings, and to return sensitive but unclassified tear-line[53] information, as

50 House Committee on Appropriations Report 108-221 (to accompany H.R. 2799), July 21, 2003.

51 FY2004 Senate Appropriations Committee Report 108-144.

52 The GIWG conducted a preliminary survey of systems/initiatives that are operational or being developed at the local, state, federal, and regional levels. Several systems/initiatives were identified. Refer to the companion CD for a list of the systems identified, as well as summary information obtained during the survey.

53 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.

appropriate, to law enforcement inquirers through the sensitive but unclassified connected systems or other means (e.g., through federal agencies or the FBI JTTFs).

The OSIS system connected to the DOS OpenNet Plus sensitive but unclassified system (43,000 users) in November 2002. Planning is under way for the DOS Bureau of Consular Affair's Consolidated Consular (visa) Database to be accessible for query by law enforcement.

DISA's ADNET-U, a system of 5,000 local, state, tribal, and federal law enforcement officials predominantly along the Southwest Border, Canada, and Latin America, was certified, accredited, and connected to OSIS in April 2003. The OSIS/OpenNet/ADNET-U connection with RISS/LEO will enable previously unavailable collaboration among law enforcement and the intelligence community at the sensitive but unclassified level.

RISS has expanded its resources and implemented RISS ATIX to provide access through RISSNET to additional groups of users for secure interagency communication, information sharing, and dissemination of terrorist threat information. Additional groups of users include public service, public safety, emergency management, utility, and other critical infrastructure personnel that have traditionally not been served by RISS. RISS ATIX participants are assigned restricted access to certain specific RISS services and resources, as appropriate, in consideration of their roles with regard to terrorism and disasters.

DHS, in conjunction with the RISS centers, has implemented a pilot project that has established a bulletin board and secure e-mail capability for communications between DHS, local and state law enforcement, and appropriate security personnel at nuclear power plants, using RISSNET. The initiative involves identification of selected critical infrastructure sites (initially a set number of nuclear power facilities), establishing liaison with local and state law enforcement agencies within the jurisdictional areas surrounding the identified facilities, reporting of suspicious activities and incidents related to the security of those facilities, and provision by DHS of analysis and feedback on those activities. The pilot project, initiated in spring 2003, involves the states of Arizona, California, Connecticut, Florida, Massachusetts, Nebraska, and Pennsylvania. The scope of the project and the nature of the critical infrastructure being monitored are expected to expand as the initiative progresses.

There are other systems and valuable applications that are currently being used by the law enforcement community. From a strategic perspective, these types of systems and initiatives should become part of the nationwide sensitive but unclassified communications capability in order to expand collaboration and information sharing opportunities across existing enterprises.

One example is the Joint Regional Information Exchange System (JRIES). JRIES was initiated as a pilot project by the DoD Defense Intelligence Agency (DIA) to improve the exchange of counterterrorism information between local and state law enforcement and components of DoD and DIA, so as to further engage law enforcement in military force and infrastructure protection at domestic U.S. military facilities. The DIA-led Joint Intelligence Task Force-Combating Terrorism (JITF-CT) has access to classified and sensitive but unclassified data and provides analysis of these data for sharing, at the sensitive but unclassified level, with law enforcement.

Initiated as a pilot project in December 2002 by JITF-CT with the New York Police Department Counterterrorism Bureau (NYPD CTB) and the California Department of Justice Anti-Terrorism Information Center (CATIC), JRIES employs collaboration and data visualization software over a secure network. JRIES reached operational status in February 2003 and now includes participation by many states, municipalities, and federal agencies, including DHS. JRIES connectivity with RISSNET was proposed but is not yet implemented, pending resolution of security and architectural compatibilities. Connectivity was also proposed for JRIES using the proposed OSIS connection to RISS/LEO. This connectivity is also not yet adopted, pending resolution of the same issues. The JRIES Executive Board is addressing these, as well as other related program governance issues.

The JRIES program sponsorship and management is currently being transferred to DHS.

With 85 percent of the nation's critical infrastructure owned and operated by the private sector, these facilities, their security personnel and systems, and the security personnel of the nation's commercial sector offer important partners with whom information and intelligence must be shared and with whom the law enforcement and homeland security communities must improve, and make routine, the means of collaboration. RISS ATIX, combined with JRIES capabilities, offers the most immediate and pervasive system to satisfy those important needs.

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.**

Discussion: Any requirement to utilize the nationwide sensitive but unclassified communications backbone, initially the RISS/LEO communications capability, will allow for the use of existing infrastructures without constraining the ability of those wanting to participate in the most timely and cost-effective manner. The nationwide sensitive but unclassified architecture will evolve to include the necessary flexibility to support fully functional bidirectional information sharing, while utilizing existing local, state, tribal, and regional infrastructure.

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.**

Discussion: Currently connected sensitive but unclassified systems must establish a common means of recognizing and accepting various access control and individual authentication methods as acceptable methods of access to the nationwide communications capability and the information resources accessible on the network and various participating systems. Currently, existing connected sensitive but unclassified systems employ the certification and accreditation processes to assess and establish the requisite trust to connect another system to the LEO and OSIS systems. System administrators and security authorities should define an "approved" set of network and system access control methods for joining systems to satisfy and meet their security, encryption, and connectivity needs so that they can recognize and provide access throughout the nationwide communications capability as if a single access method has been employed.

As the recommended initial communications backbone, the RISS/LEO interconnection is able to connect to several unclassified systems throughout the United States. For instance, the Florida Department of Law Enforcement's state system and Iowa's Law Enforcement Intelligence Network, commonly known as LEIN, are both connected as nodes to RISSNET.

In addition to Florida and Iowa, ten other state law enforcement networks are connected as nodes to RISSNET, including California, Colorado, Missouri, New York, Oregon, Pennsylvania, South Dakota, Utah, Washington, and Wyoming. Recently, the Commissioner of the Minnesota Department of Public Safety agreed to examine connecting the state and local law enforcement component of the CriMNet network (see footnote 47b) as a node on RISSNET. Additionally, RISSNET node connections are pending for the following states: Arizona, Connecticut, Delaware, Georgia, Hawaii, Michigan, Nebraska, Ohio, and Tennessee.

In a variation on that theme, the CISA Network (CISAnet),[54] serving state and local law enforcement organizations in six states (Arizona, California, Georgia, Idaho, New Mexico, and Texas), is connected through a trusted gateway to the six RISS centers and the DEA's El Paso Intelligence Center (EPIC) in Texas. This is a system-to-system connection that established fully operational capabilities in late 1996 based on trust relationships and honest broker agreements that provide real-time bidirectional query access to data and does not require that CISAnet employ the RISSNET authentication and encryption software and hardware.

Similarly to that approach, the Justice Consolidated Office Network of DOJ employs the RISSGate VPN software, but not the RISSNET smart card and companion card-reader hardware, to authenticate and encrypt Internet sessions initiated to RISS and LEO. The 94 U.S. Attorneys' Offices are connecting to RISSNET.

A recently developed project, supported by DOJ and DHS funding, will rely on the existing RISSNET communications network. The MATRIX pilot project was initiated in response to the increased need for timely information sharing and exchange of terrorism-related information among members of the law enforcement community. The MATRIX pilot project includes three primary objectives: using factual data analysis from existing data sources and data integration technology to improve the usefulness of information contained in multiple types of document storage systems, providing a mechanism for states to become nodes on RISSNET for electronic exchange among participating agencies, and encouraging the exchange of information via secure state Web sites. Several states[55] are participating in the pilot project, and it is hoped that the project will be expanded nationwide once the concept is further documented.

54 The Criminal Information Sharing Alliance Network (CISAnet) is the former Southwest Border States Anti-Drug Information System (SWBSADIS) begun in 1992 when the initiating states requested support from the federal government to share law enforcement information. It received funding from the U.S. Department of Defense (DoD); Defense Information Systems Agency (DISA); and the U.S. Department of Justice (DOJ), National Institute of Justice, the DOJ's research and development office. CISAnet is now funded by the Congress through DOJ, Bureau of Justice Assistance, and DoD and administered by DISA.

55 The states participating in the MATRIX pilot are Connecticut, Florida, Georgia, Michigan, New York, Ohio, Pennsylvania, and Utah.

Recommendation 25: Agencies participating in the *National Criminal Intelligence Sharing Plan* are encouraged to use *Applying Security Practices to Justice Information Sharing*[56] as a reference document regarding information system security practices. The document was developed by the Global Security Working Group (GSWG) 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.

Discussion: Modern justice agencies rely heavily upon their IT resources to perform critical tasks and to provide emergency services to the public. Increasingly, justice agencies share information across wide-area networks and the Internet. The sensitivity of this information and its related systems infrastructure make it a particularly vulnerable target. Because of its importance, sharing itself requires a technological environment, intended and trusted to keep information safe from unauthorized exposure.

LEO, RISS, OSIS, OpenNet, and ADNET-U systems have defined security practices and accreditation and certification criteria for participation in their systems. Likewise, local and state sensitive but unclassified systems have security standards for employing Internet and intranet connectivity.

In May 2002, the GSWG recognized the increased emphasis on security practices to ensure trusted information sharing and has since developed the document *Applying Security Practices to Justice Information Sharing*. In July 2003, the GSWG formed a Systems Security Compatibility Task Force, comprised of local, state, tribal, and federal representatives. The group's mission is to establish security priorities, policies, and guidelines to achieve system-wide compatibility for justice and public safety information sharing without compromising security.

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)[57] 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.

Discussion: Extensible Markup Language, or "XML" as it is commonly referenced, was developed out of the standard generalized markup language (a page definition and formatting language). XML is sanctioned by the World Wide Web Consortium (www.W3.org) to define a way of transmitting and representing data. XML is designed to transmit data and the meaning of the data. This is accomplished by allowing data "tags" to define both the name of a data element and the format of the data within that element. XML also allows structured relationships to be defined; for example, one named person (subject) in the database might have multiple street addresses and multiple criminal associates, all of which XML is capable of recognizing, revealing, and communicating as "relationships."

XML is easily transmitted as text over the current Internet infrastructure. It is compatible with major Internet transmission protocols and is also highly compressible for faster transmission. Major database vendors and their database applications provide software development "tools" to assist justice agency technical staff to develop and use XML more efficiently and productively within agency applications. XML is very developer-friendly, yet ordinary users with no particular XML expertise can make sense of an XML file. The XML standard is designed to be independent of vendor, operating system, source application, destination application, storage medium, and/or transport protocol.

In August 2002, the Global Infrastructure/Standards Working Group, XML Committee formed the Global XML Structure Task Force (GXSTF) to identify data requirements, explore XML concepts, and apply XML best practices to design and implement a Global JXDD. The GXSTF is composed of government and industry domain experts (from law enforcement, courts, and corrections), technical managers, and engineers. The Global JXDD is an object-oriented data model, database, and XML-schema specification that represents the semantics and structure of common data elements and types required to consistently exchange information within the justice and public safety communities. The GXSTF is developing technical compliance criteria to facilitate interoperability of the Global JXDD. These criteria can be referenced in requests for proposals and grant conditions in order to support consistent and interoperable implementations.

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

56 This document is available at: http://www.it.ojp.gov/global/.

57 The latest version of the Global JXDM and the Global JXDD is included on the companion CD and can be found at: http://www.it.ojp.gov/jxdm.

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.

Discussion: Issues of trust continue to undermine information sharing efforts between all levels of law enforcement. Information security is primarily a factor of the individuals who have access to the information. The trust relationship needed for criminal intelligence sharing is founded, in part, on the integrity of the individuals with whom information is shared. That integrity can be assessed, in part, through stringent membership vetting procedures of both the individuals involved and their parent agencies. To promote use of the nationwide communications capability and the sharing of criminal information and intelligence in a meaningful level of detail and completeness, a greater level of stringency membership criteria is recommended for individuals desiring access to the sensitive but unclassified communications capability for law enforcement purposes.

The background name check recommended for access to the sensitive but unclassified communications capability does not include or require a field investigation component, as is required for law enforcement employment in many jurisdictions and at the federal level, for national security clearances and for law enforcement employment suitability determinations, such as that for public trust (high-risk) positions. The recommendation for a fingerprint-based records check, followed by a name check every three years thereafter, is the minimum standard suggested; more stringent background criteria imposed by agencies are not discouraged.

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. The CICC will submit a report on these tools to OJP by June 30, 2004.**

Discussion: Participants in the IACP Criminal Intelligence Sharing Summit stressed that law enforcement officers' training and continuing education must equip relevant personnel to use new technologies that complement or facilitate intelligence sharing. Mechanisms must be developed that enable local law enforcement agencies, including those with limited resources, to participate in intelligence development and sharing and to practice intelligence-led policing.

Consideration should be given to generically identifying the types of products available (in lieu of identifying the vendor). A current list of product users should be recommended as resources for those agencies that are in the market for analytical tools. Categories of analytical tools will be identified (open source, data mining, crime information, trend analysis, visualization and collaboration methods, link analysis, Geographic Information Systems mapping, etc.) and a standard "tool set" of these products will be recommended to utilize as a resource for sharing tools among groups of users. A listing of the various available products, as well as a list of users, can be disseminated using various mechanisms, including Web sites, publications, and training sessions.

Appendix A: 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.

Counterintelligence – Information compiled, analyzed, and/or disseminated in an effort to investigate espionage, sedition, subversion, etc., that is 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 within 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 Element – A field within a database that describes or defines a specific characteristic or attribute.

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

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/Reevaluation – 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 *Intelligence 2000: Revising the Basic Elements*, 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 is 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 – Indicates that 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.

Predicate – The basis for the initiation of any inquiry or investigation.

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.

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

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)

Reasonable Suspicion – When information exists that 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, p. vi)

Restricted Data – Reports that at an earlier date were classified sensitive or confidential with the need for high-level security no longer existing.

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.)

Secret – Applied to information of which the unauthorized disclosure could reasonably be expected to cause serious damage to national security.

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 that 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 that 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)

Top Secret – Applied to information of which the unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security.

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 that 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 B: Acronyms

ADNET-U	Anti-Drug Network-Unclassified
AES	Advanced Encryption Standard
ARJIS	Automated Regional Justice Information System
ATIX	Automated Trusted Information Exchange
BJA	Bureau of Justice Assistance
CATIC	California Anti-Terrorism Information Center
CDICG	Counterdrug Intelligence Coordination Group
CDX	Counterdrug Intelligence Executive Secretariat
CFR	Code of Federal Regulations
CICC	Criminal Intelligence Coordinating Council
CIO	Chief Information Officer
CISAnet	Criminal Information Sharing Alliance Network
CJIS	Criminal Justice Information Services
CLEAR	Chicago Citizen and Law Enforcement Analysis and Reporting
COP	Community Oriented Policing
DEA	U.S. Drug Enforcement Administration
DES	Triple-Data Encryption Standard
DHS	U.S. Department of Homeland Security
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DoD	U.S. Department of Defense
DOJ	U.S. Department of Justice
DOS	U.S. Department of State
FBI	Federal Bureau of Investigation
FOUO	"For Official Use Only" information handling caveat
GAC	Global Justice Information Sharing Initiative Advisory Committee
GISWG	Global Justice Information Sharing Initiative Infrastructure/Standards Working Group
GIWG	Global Justice Information Sharing Initiative Intelligence Working Group
Global	Global Justice Information Sharing Initiative
GSWG	Global Justice Information Sharing Initiative Security Working Group
HIDTA	High Intensity Drug Trafficking Areas
IACP	International Association of Chiefs of Police
IADLEST	International Association of Directors of Law Enforcement Standards and Training
IAFIS	Integrated Automated Fingerprint Identification System
IALEIA	International Association of Law Enforcement Intelligence Analysts
III	Interstate Identification Index
ISI	Gateway Information Sharing Initiative
IT	Information Technology
JCON	Justice Consolidated Office Network
JITF-CT	Joint Intelligence Task Force-Combating Terrorism
JRIES	Joint Regional Information Exchange System
LEADS	Law Enforcement Agency Data System

LEIN	Law Enforcement Intelligence Network
LEIU	Law Enforcement Intelligence Unit
LEO	Law Enforcement Online
LES	"Law Enforcement Sensitive" information handling caveat
MATRIX	Multistate Anti-Terrorism Information Exchange
NAS	National Alert System
NCIC	National Crime Information Center
NDIC	National Drug Intelligence Center
NDPIX	National Drug Pointer Index
NICS	National Instant Criminal Background Check System
NIPRNET	Unclassified but Sensitive Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NLETS	International Justice and Public Safety Information Sharing Network
NSA	National Sheriffs' Association
NW3C	National White Collar Crime Center
NYPD CTB	New York Police Department Counterterrorism Bureau
OJP	Office of Justice Programs
OSIS	Open Source Information System
RISS	Regional Information Sharing Systems
RISSNET	Regional Information Sharing Systems secure intranet
SIG	Special-Interest Groups
SPPADS	State and Provincial Police Academy Directors Section
SWBSADIS	Southwest Border States Anti-Drug Information System
UCR	Uniform Crime Reporting
VPN	Virtual Private Network
W3	World Wide Web Consortium
XML	Extensible Markup Language

Appendix C: Sources

Bureau of Justice Assistance, *Criminal Intelligence System Operating Policies* (28 Code of Federal Regulations Part 23.20). 1993.

California Department of Justice, *The Bureau of Intelligence Operations Manual*. 1993.

California Peace Officers' Association, *Criminal Intelligence Program for the Smaller Agency*. 1988.

Davis, Kenneth Culp, *Discretionary Justice: A Preliminary Inquiry*. 1971.

Europol, *Analytical Guidelines*. 2000.

Goldstein, Herman, "Controlling and Reviewing Police-Citizen Contacts," *Policing a Free Society*. 1977.

Gottlieb, Steven, Raj Singh, and Shel Arenberg, *Crime Analysis: From First Report to Final Arrest*. Alpha Publishing, 1995.

Grabo, Cynthia M., *Warning Intelligence*. Association of Former Intelligence Officers, 1987.

Harris, Don R., and E. Drexel Godfrey, *The Basic Elements of Intelligence*. Law Enforcement Assistance Administration, 1971.

Harris, Don R., et al., *The Basic Elements of Intelligence*, 2nd edition. Law Enforcement Assistance Administration, 1976.

International Association of Chiefs of Police, National Law Enforcement Policy Center. *Criminal Intelligence*. 1998.

_____ , *Law Enforcement Policy on the Management of Criminal Intelligence*. 1985.

INTERPOL, *Crime Analysis Booklet*. International Criminal Police Organization Crime Analysis Working Group, 1996.

Krizan, Lisa, *Intelligence Essentials for Everyone*. Joint Military Intelligence College, 1999.

LaFave, Wayne, *Arrest*. 1965.

McDowell, Donald, *Strategic Intelligence*. Istana Enterprises, 1998.

Morris, Jack, and Charles Frost, *Police Intelligence Reports*. Palmer Press, 1983.

National Criminal Intelligence Service UK, *The National Intelligence Model*. 2001.

National Criminal Justice Association, *Justice Information Privacy Guideline: Developing, Drafting, and Assessing Privacy Policy for Justice Information Systems*. 2002.

Peterson, Marilyn B., *Applications in Criminal Analysis*. Greenwood Press, 1994.

Peterson, Marilyn B., Bob Morehouse, and Richard Wright (Eds.), *Intelligence 2000: Revising the Basic Elements*. LEIU and IALEIA, 2001.

Prunckun, Henry W., Jr., *Special Access Required*. Scarecrow Press, 1990.

Smith, Angus (Ed.), *Intelligence-Led Policing*. IALEIA, 1997.

Warren, Samuel, and Louis Brandeis, "The Right to Privacy," *Harvard Law Review*. 1890.

Appendix D

Core 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 in 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 developing 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 was to identify specific training topics and issues for each level of personnel involved in the intelligence process. Their second goal was 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 that are noncommercial-based and associated with reputable and knowledgeable organizations. During the research phase, the Committee noted the lack of national-level training standards and an absence of any single national agency coordinating intelligence training.

Local, state, and federal governmental agencies as well as private/nonprofit 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 compile it into a cohesive training package.

Global Intelligence Working Group 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 the Training Committee recognizes the difficulties associated with the implementation and subsequent delivery of a suggested training for local and state law enforcement officers.

It is imperative that all Peace Officer Standards and Training (POST) Commissions of this nation 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.

Level One Law Enforcement Officers

Role
The role of law enforcement officers, relative to intelligence, is to be cognizant that 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.

Level Two Law Enforcement Executives

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 chief 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 its role played 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.

Level Three Intelligence Commanders/ Supervisors

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.

Level Four Intelligence Officers/ Collectors

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.

Level Five — Intelligence Analysts

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.

Level Six — Train-the-Trainer

Role
It is necessary to train people to deliver the different levels of courses before they can be provided, particularly for Levels Three and Four. (Levels One and Two are a one-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 from a variety of sources 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 examples of 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
A train-the-trainer class 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.

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 Areas Assistance Center, "Analysis and Critical Thinking"; as well as California and Arizona POST[58] Board curricula. A listing of available intelligence training sources and specifically scheduled classes is found on the IALEIA Web site, www.ialeia.org. This listing is updated on a semiannual basis and also allows individuals to directly contact training source agencies and organizations for more information on classes and schedules.

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.

58 For more information, see the California POST Web site, www.post.ca.gov, and the Arizona POST Web site, www.azpost.state.az.us.

"I am pleased to announce that I have just approved the National Intelligence Sharing Plan, a direct result of recommendations made at the IACP Summit held in March of 2002. With the Plan formally in place, we can build on the communication, coordination, and cooperation that are winning the fight against crime and the war against terror."

John Ashcroft
Former U.S. Attorney General

"Critical to preventing future terrorist attacks is improving our intelligence capability. The Plan will serve as a blueprint as we continue to develop our overall national strategy for sharing information."

Robert Mueller
Director, Federal Bureau of Investigation

"...We must create new ways to share information and intelligence both vertically, between governments, and horizontally, across agencies and jurisdictions...efforts with the Global Intelligence Working Group to create a National Criminal Intelligence Sharing Plan...a helpful and welcome response."

Tom Ridge
Former Secretary, U.S. Department of Homeland Security

Third Printing 07/05