U.S. Department of Justice
Office of Justice Programs
Bureau of Justice Assistance

NEW REALITIES
Law Enforcement in the Post-9/11 Era

Intelligence-Led Policing: The New Intelligence Architecture

BJA Bureau of Justice Assistance

U.S. Department of Justice
Office of Justice Programs
810 Seventh Street NW.
Washington, DC 20531

Alberto R. Gonzales
Attorney General

Regina B. Schofield
Assistant Attorney General

Domingo S. Herraiz
Director, Bureau of Justice Assistance

Office of Justice Programs
Partnerships for Safer Communities
www.ojp.usdoj.gov

Bureau of Justice Assistance
www.ojp.usdoj.gov/BJA

NCJ 210681

Written by Marilyn Peterson

This document was prepared by the International Association of Chiefs of Police under cooperative agreement number 2003–DD–BX–K002 awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. 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.

The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime.

Intelligence-Led Policing: The New Intelligence Architecture

September 2005

NCJ 210681

BJA *Bureau of Justice Assistance*

Acknowledgments

Post-9/11 Policing Project Staff

The Post-9/11 Policing Project is the work of the International Association of Chiefs of Police (IACP), National Sheriffs' Association (NSA), National Organization of Black Law Enforcement Executives (NOBLE), Major Cities Chiefs Association (MCCA), and Police Foundation. Jerry Needle, Director of Programs and Research, IACP, provided overall project direction.

- **International Association of Chiefs of Police**

  Phil Lynn served as IACP's Project Director, managed development and publication of the four Promising Practices Briefs, and authored *Mutual Aid: Multijurisdictional Partnerships for Meeting Regional Threats.* Andrew Morabito coauthored *Engaging the Private Sector To Promote Homeland Security: Law Enforcement-Private Security Partnerships,* and analyzed Post-9/11 survey data. Col. Joel Leson, Director, IACP Center for Police Leadership, authored *Assessing and Managing the Terrorism Threat.* Walter Tangel served as initial Project Director.

  Dr. Ellen Scrivner, Deputy Superintendent, Bureau of Administrative Services, Chicago Police Department, contributed to all phases of project design and cofacilitated the Post-9/11 Roundtables with Jerry Needle. Marilyn Peterson, Management Specialist–Intelligence, New Jersey Division of Criminal Justice, authored this monograph—*Intelligence-Led Policing: The New Intelligence Architecture.*

- **National Sheriffs' Association**

  Fred Wilson, Director of Training, directed NSA project activities, organized and managed Post-9/11 Roundtables, and worked closely with IACP staff throughout the course of the project. NSA project consultants included Chris Tutko, Director of NSA's Neighborhood Watch Project; John Matthews; and Dr. Jeff Walker, University of Arkansas, Little Rock.

- **National Organization of Black Law Enforcement Executives**

  Jessie Lee, Executive Director, served as NOBLE's Project Director and conducted most staff work.

- **Major Cities Chiefs Association**

  Dr. Phyllis McDonald, Division of Public Safety Leadership, Johns Hopkins University, directed the work of the Major Cities Chiefs Association. The MCCA team included Denis O'Keefe, Consultant; Corinne Martin, Program Coordinator; and Shannon Feldpush.

  Dr. Sheldon Greenberg, Director of the Division of Public Safety Leadership, coauthored *Engaging the Private Sector To Promote Homeland Security: Law Enforcement-Private Security Partnerships.*

- **The Police Foundation**

  Edwin Hamilton directed Police Foundation project activities and managed Post-9/11 survey formatting and analysis, assisted by Rob Davis. Foundation consultants included Inspector Garth den Heyer of the New Zealand Police and Steve Johnson of the Washington State Patrol.

Promising Practices Reviews

Promising Practices drafts were critiqued and enriched by a series of practitioners/content experts, including Richard Cashdollar, Executive Director of Public Safety, City of Mobile, AL; George Franscell, Attorney-at-Law, Franscell, Strickland, Roberts and Lawrence, Los Angeles, CA; Mary Beth Michos, State Mutual Aid Coordinator, Prince William County, VA; David Bostrom, Manager, Community Policing Consortium, IACP; John P. Chase, Chief of Staff, Information Analysis and Infrastructure Protection, Department of Homeland Security; John M. Clark,

Assistant Vice President/Chief of Police, Burlington Northern Santa Fe Railroad; John A. LeCours, Director/Intelligence, Transport Canada; Ronald W. Olin, Chief of Police, Lawrence, KS; Ed Jopeck, Analyst, Veridian; Jerry Marynik, Administrator, State Terrorism Threat Assessment Center, California Department of Justice; and Bart Johnson, Office of Counter-Terrorism, New York State Police.

Executive Oversight

The Post-9/11 Policing Project was initially conceptualized by the Office of Justice Programs, U.S. Department of Justice. Since its inception, the project has been guided throughout by the chief executive officers of the partner associations:

- Daniel N. Rosenblatt, Executive Director, International Association of Chiefs of Police
- Thomas N. Faust, Executive Director, National Sheriffs' Association
- Jessie Lee, Executive Director, National Organization of Black Law Enforcement Executives
- Thomas C. Frazier, Executive Director, Major Cities Chiefs Association
- Hubert Williams, President, The Police Foundation

Bureau of Justice Assistance Guidance

We gratefully acknowledge the technical guidance and patient cooperation of executives and program managers who helped fashion project work: James H. Burch II, Deputy Director; Michelle Shaw, Policy Advisor; and Steven Edwards, Ph.D., Senior Policy Advisor for Law Enforcement.

Contents

Executive Summary

The terrorist attacks of September 11, 2001 revealed the life-and-death importance of enhancing U.S. intelligence operations. Since that day, a tremendous amount of attention has been focused on the need for constructive changes in law enforcement intelligence.

Intelligence operations have been reviewed, studied, and slowly but steadily transformed. Most efforts have focused on reorganizing intelligence infrastructures at the federal level; however, corresponding efforts have been made to enhance state and local law enforcement intelligence operations. Such enhancements make it possible for state and local law enforcement agencies to play a role in homeland security. Perhaps more important, improvements to intelligence operations help local law enforcement respond to "traditional" crimes more effectively.

Because effective intelligence operations can be applied equally well to terrorist threats and crimes in the community, homeland security and local crime prevention are not mutually exclusive. Officers "on the beat" are an excellent resource for gathering information on all kinds of potential threats and vulnerabilities. However, the intelligence operations of state and local law enforcement agencies often are plagued by a lack of policies, procedures, and training for gathering and assessing essential information.

To correct this problem, fundamental changes are needed in the way information is gathered, assessed, and redistributed. Traditional, hierarchical intelligence functions need to be reexamined and replaced with cooperative, fluid structures that can collect information and move intelligence to end users more quickly. Intelligence in today's policing environment must adapt to the new realities presented by terrorism and conventional crimes.

These new realities require increased collaboration in information gathering and intelligence sharing. Critical community infrastructures such as those related to food, agriculture, public health, telecommunications, energy, transportation, and banking are now seen as potential terrorist targets. As a result, parts of the community that previously did not receive much notice from state and local law enforcement agencies now require keen attention. Personnel who work in these and other key industries are now partners in terrorism prevention and crime control. Similarly, community- and problem-oriented policing must be integrated into intelligence operations to address conventional crime issues. Engaging and collaborating with the community at all levels are essential.

Intelligence-led policing is a collaborative enterprise based on improved intelligence operations and community-oriented policing and problem solving, which the field has considered beneficial for many years. To implement intelligence-led policing, police organizations need to reevaluate their current policies and protocols. Intelligence must be incorporated into the planning process to reflect community problems and issues. Information sharing must become a policy, not an informal practice. Most important, intelligence must be contingent on quality analysis of data. The development of analytical techniques, training, and technical assistance needs to be supported.

Because of size and limited budgets, not all agencies can employ intelligence analysts or intelligence officers. Nonetheless, all law enforcement agencies have a role in the transformation of national intelligence operations. This document identifies four levels of intelligence capabilities for state and local agencies. At each level, steps can be taken to help agencies incorporate intelligence-led policing strategies. These steps include adopting mission statements, writing intelligence policies and procedures, participating in information sharing, establishing appropriate security, and adopting legal safeguards to protect the public's privacy and civil liberties.

More than 20 years ago, some in law enforcement argued for similar changes and an expanded application of intelligence operations. A national catastrophe was required to confirm the wisdom of their call. Their plea, espoused years ago, is even more urgent today. “Law enforcement administrators,” they said, “can no longer afford to respond to contemporary and future problems with the ‘solutions’ of yesterday.”[1]

Introduction

A critical lesson taken from the tragedy of September 11, 2001 is that intelligence is everyone's job. A culture of intelligence and collaboration is necessary to protect the United States from crimes of all types. Likewise, for intelligence to be effective, it should support an agency's entire operation. Crime prevention and deterrence must be based on all-source information gathering and analysis.

However, not all agencies have the resources to mount full-scale intelligence operations. The average city police department in the United States had 41 sworn personnel in 2001[2] and would not be expected to have intelligence analysts on staff. How then can an intelligence model be established that will provide support for all agencies?

The needs of agencies—from the very small to the very large—must be considered if intelligence-led policing is to be established in the United States. This document examines how law enforcement agencies can enhance their intelligence operations for homeland security and traditional enforcement and crime prevention, regardless of how sophisticated their intelligence operations are. It explores the meaning and uses of intelligence, provides examples of intelligence practices, and explores how to establish and maintain an intelligence capability.

Intelligence Issues

Introducing intelligence-led policing into U.S. law enforcement agencies is problematic for several reasons. First, many agencies do not understand what intelligence is or how to manage it. Second, agencies must work to prevent and respond to day-to-day crime at the same time they are working to prevent terrorism. Third, the realities of funding and personnel resources are often obstacles to intelligence-led policing. Although the current intelligence operations of most law enforcement agencies prevent them from becoming active participants in the intelligence infrastructure, this problem is not insurmountable.

What Is Intelligence?

Because of misuse, the word "intelligence" means different things to different people. The most common mistake is to consider "intelligence" as synonymous with "information." Information is not intelligence. Misuse also has led to the phrase "collecting intelligence" instead of "collecting information." Although intelligence may be collected by and shared with intelligence agencies and bureaus, field operations generally collect information (or data).

Despite the many definitions of "intelligence" that have been promulgated over the years, the simplest and clearest of these is "information plus analysis equals intelligence."

The formula above clarifies the distinction between collected information and produced intelligence. It notes that without analysis, there is no intelligence. Intelligence is not what is collected; it is what is produced after collected data is evaluated and analyzed.

Intelligence is not what is collected; it is what is produced after collected data is evaluated and analyzed.

If intelligence is analyzed information, what is analysis? Some agencies contend that computer software can perform analysis for them; thus, they invest in technology rather than in trained analysts. However, analysis requires thoughtful contemplation that results in conclusions and recommendations. Thus, computers may assist with analysis by compiling large amounts of data into an easily accessible format, but this is only collated data; it is not analyzed data or information, and it falls far short of intelligence. For information to be useful, it must be analyzed by a trained intelligence professional. In other words, intelligence tells officials everything they need to know before they knowledgeably choose a course of action. For example, intelligence provides law enforcement executives with facts and alternatives that can inform critical decisions.

Tactical Intelligence Versus Strategic Intelligence

The distinction between tactical and strategic intelligence is often misconstrued. Tactical intelligence contributes directly to the success of specific investigations. Strategic intelligence deals with "big-picture" issues, such as planning and manpower allocation.[3] Tactical intelligence directs immediate action, whereas strategic intelligence evolves over time and explores long-term, large-scope solutions.

Some professionals refer to "evidential intelligence," in which certain pieces of evidence indicate where other evidence may be found.[4] Evidential intelligence can help prove a criminal violation or provide leads for investigators to follow.[5]

The term "operational intelligence" is sometimes used to refer to intelligence that supports long-term investigations into multiple, similar targets. Operational intelligence is concerned primarily with identifying, targeting, detecting, and intervening in criminal activity.[6]

Why Intelligence Is Critical

Intelligence is critical for decisionmaking, planning, strategic targeting, and crime prevention. Law enforcement agencies depend on intelligence operations

on all levels; they cannot function effectively without collecting, processing, and using intelligence.

Decisionmaking

Gathering information and deciding what to do with it are common occurrences in law enforcement operations. Law enforcement officers and managers are beset by large quantities of information, yet decisions are often based on information that may be incomplete, inaccurate, or misdirected. The move from information gathering to informed decisionmaking depends on the intelligence/analytic process, and results in a best estimate of what has happened or will happen.

Questions have been asked about the extent to which substantive analysis was performed prior to September 11 to test hypotheses of attacks by foreign terrorist groups against the United States, and whether domestic agencies were told to assess these threats or to develop a plan of action and present it to decisionmakers. It appears that decisionmakers relied on raw intelligence reports that may have raised concerns but did not guide informed decisions.

Experience shows that intelligence and analysis must be strengthened to meet the threat of terrorism against the United States. Law enforcement personnel have a key role to play in making this happen.

Planning

Intelligence is critical to effective planning and subsequent action. In many law enforcement agencies, planning is performed without an understanding of the crime problems facing the jurisdiction and without sufficient operational input. In these instances, strategic planning bears no resemblance to strategic analysis or strategic intelligence. Instead, it relates only to funding issues and operational constraints. Essentially a budget exercise, this type of planning suffers from a disconnect between the major issues facing a community and the manner in which funds are spent to address those needs.

Law enforcement executives are being encouraged to view policing as a business. The United Kingdom's *National Intelligence Model* notes that:

> *The law enforcement business is about the successful management and reduction of crime and other law enforcement problems. . . . The vital central ingredient in successful planning is identification and understanding*
>
> - *an accurate picture of the business,*
> - *what is actually happening on the ground,*
> - *the nature and extent of the problem,*
> - *the trends, and*
> - *where the main threats lie.*[7]

Law enforcement executives are being encouraged to view policing as a business.

By adhering to these principles, commanders can create responsive enforcement plans that meet the needs of the community. This cannot be done through sheer managerial vision. It must be embedded in critical thinking based on intelligence and analysis.

Strategic Targeting

Strategic targeting and prioritization are other critical roles of intelligence. Law enforcement agencies with tight budgets and personnel reductions or shortages must use their available resources carefully, targeting individuals, locations, and operations that promise the greatest results and the best chances for success. Case or lead overloads can reduce investigators' efficiency unless they know how to identify the most fruitful leads. Intelligence enables officers to work more efficiently.

For example, to help fight terrorism and domestic extremism, the California Department of Justice examines group characteristics, criminal predicates, target analyses, and intervention consequences to determine which groups pose the greatest threat to the state.[8] By reviewing and comparing this information, the agency can prioritize which groups require the earliest intervention. In addition, response strategies can be selected based on an understanding of the group's activities and an awareness of what resources are available.

Crime Prevention

The final area in which intelligence is critical is crime prevention. Using intelligence from previous crimes in local and other jurisdictions, indicators can be created and shared among law enforcement agencies. Comparing the indicators from local neighborhoods, analysts can anticipate crime trends and agencies can take preventive measures to intervene or mitigate the impact of those crimes.

How We Got Where We Are Today: An Overview of Intelligence History

Law enforcement intelligence is an outgrowth of military and national security intelligence. Military intelligence dates back to ancient times; references to it can be found in Chinese writings (Sun Tzu) and the Bible (Numbers 13). Security intelligence was adapted for use in law enforcement operations after World War II. Today, communications intelligence methods used by the military influence how law enforcement analyzes telephone records, and techniques used to manage human intelligence sources inform the management of confidential informants.

The original blueprint for intelligence work was published by the Law Enforcement Assistance Administration of the U.S. Department of Justice in 1971. In 1973, the National Advisory Commission on Criminal Justice Standards and Goals made a strong statement about intelligence. It called on every law enforcement agency and every state to immediately establish and maintain the capability to gather and evaluate information and to disseminate intelligence in a manner that protects every individual's right to privacy while it curtails organized crime and public disorder.[9]

The standards went on to note that every state should establish a "central gathering, analysis and storage capability, and intelligence dissemination system" in which law enforcement agencies participate by providing information and receiving intelligence from the system. It further stated that every agency with more than 75 personnel should have a full-time intelligence capability.[10]

When first instituted, intelligence units within law enforcement departments were not governed by policies that protected civil liberties and prevented intelligence excesses. During the 1970s, a number of intelligence units ran afoul of good practices, and, as a result, some agencies shut down their intelligence functions voluntarily, by court order, or from political pressure. In 1976, in response to the problem of intelligence abuses, standards were developed that required a criminal predicate for subjects to be entered in criminal intelligence files. During this time, the Law Enforcement Intelligence Unit (LEIU) *File Guidelines* were developed, along with those of the California Department of Justice and the New Jersey State Police.

Between the late 1970s and the turn of the century, major intelligence initiatives were underway. Some of these initiatives, such as the Regional Information Sharing Systems (RISS) centers, did not even use the term "intelligence." The primary basis for intelligence sharing in the 1980s and 1990s was the *Criminal Intelligence System Operating Policies* (28 C.F.R. Part 23), which was written to apply to the RISS centers. By 2004, more than 7,100 agencies or agency branches were members of the nationwide RISS network.

When the RISS centers were being developed in 1980, the International Association of Law Enforcement Intelligence Analysts (IALEIA) was formed. Its annual meetings were held in conjunction with those of the International Association of Chiefs of Police (IACP). The 1990s saw the creation of several federal centers to support intelligence and information sharing. The National Drug Intelligence Center (NDIC) was established in Johnstown, Pennsylvania, and the Financial Crimes Enforcement Network (FinCEN) was formed in northern Virginia. Both had tactical and strategic intelligence responsibilities. Concurrently, the High Intensity Drug Trafficking Areas (HIDTAs) system was formed as a model of federal, state, and local cooperative efforts and information sharing.

A month after September 11, 2001, the Investigative Operations Committee of IACP recommended to its leadership that an Intelligence Sharing Summit be held in March 2002. The summit was attended by more than 100 intelligence experts representing federal, state, local, and tribal law enforcement from the United States and Europe. Summit attendees examined the General Criminal Intelligence Plan and the United Kingdom's National Intelligence Model (NCIS 2000) as potential blueprints for intelligence-led policing in the United States.

Key recommendations from the IACP summit were as follows:

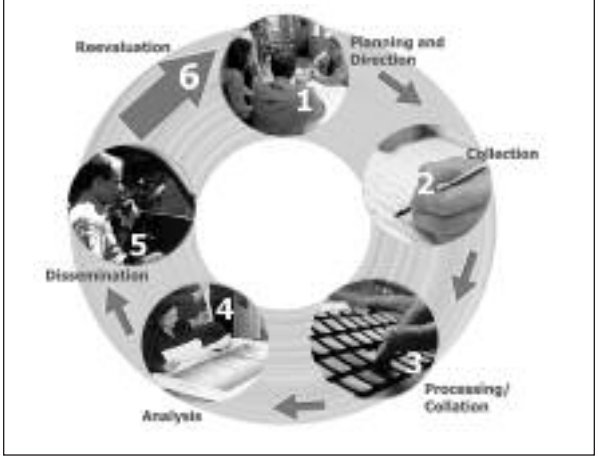
- Promote intelligence-led policing.
- Provide the critical counterbalance of civil rights.
- Increase opportunities for building trust.
- Remedy analytic and information deficits.
- Address training and technology issues.

The primary outgrowth of the summit was the creation of the Global Intelligence Working Group (GIWG), which comprises approximately 30 intelligence professionals. GIWG met quarterly during 2003 and developed the *National Criminal Intelligence Sharing Plan (NCISP)*, which was released and approved by the U.S. Attorney General in October 2003. *NCISP* contained 28 recommendations for major changes in how policing is approached. Where appropriate, those recommendations appear in this document.

Understanding the Intelligence Process

NCISP categorizes the intelligence process according to six steps: planning and direction, collection, processing/collation, analysis, dissemination, and reevaluation (see figure 1).

Figure 1. The Intelligence Process



Planning and Direction

Planning how data will be collected is key to the intelligence process. Effective planning assesses existing data and ensures that additional data collected will fill any gaps in the information already on file. As one federal manager put it, "Don't tell me what I know; tell me what I don't know."

To be effective, intelligence collection must be planned and focused; its methods must be coordinated, and its guidelines must prohibit illegal methods of obtaining information.[11] Inaccurate collection efforts can result in a flawed result, regardless of the analytical skills employed.

Planning and collection are a joint effort that requires a close working relationship between analysts, who understand how to manage, compile, and analyze information, and intelligence officers, who know the best ways to obtain information.

Planning requires an agency to identify the outcomes it wants to achieve from its collection efforts. This identification directs the scope of the officers' and agents' investigations—for example, a straightforward inquiry to identify crime groups operating in a jurisdiction or a more complex inquiry to determine the likelihood that criminal extremists will attack a visiting dignitary.

Collection

Intelligence analysis requires collecting and processing large amounts of information.[12] Data collection is the most labor-intensive aspect of the intelligence process. Traditionally, it has been the most emphasized segment of the process, with law enforcement agencies and prosecutors dedicating significant resources to gathering data. New technology and new or updated laws have supported this emphasis.

Historically, the following have been the most common forms of data collection used in intelligence units:

- Physical surveillance (either in person or by videotape).
- Electronic surveillance (trap and trace or wiretap).
- Confidential informants.
- Undercover operators.
- Newspaper reports (now also Internet sources).
- Public records (e.g., deeds, property tax records).

Today many other overt and covert sources are available. Contact information for some organizations and commercial databases are available in the appendixes.

Processing/Collation

Processing/collation involves sifting through available data to eliminate useless, irrelevant, or incorrect information and to put the data into a logical order. This organization makes it easier to identify relationships among entities and uncover relevant information.[13] Today, collation is performed using sophisticated databases with text-mining capabilities.

Database design is critical for retrieving and comparing data. Many computer software companies offer database products, but most require fine-tuning to tailor them to law enforcement agencies' needs. Smaller agencies often use "off-the-shelf" software to reduce costs. Fortunately, technology now allows different databases to interact through text-mining features.

Processing and collation also involve evaluating the data being entered. Information placed into an intelligence file is evaluated for the validity of the information and the reliability of its source.

Information placed into an intelligence system must meet a standard of relevance—i.e., it must be relevant to criminal activity associated with the informant (28 C.F.R. Part 23.20.a.).

Analysis

Analysis converts information into intelligence. As one authority on the subject notes, "Without the explicit performance of this function [analysis], the intelligence unit is nothing but a file unit."[14]

Analysis is quite simply a process of deriving meaning from data. The analytic process tells what information is present or missing from the facts or evidence. In law enforcement intelligence operations, data are analyzed to provide further leads in investigations, to present hypotheses about who committed a crime or how it was committed, to predict future crime patterns, and to assess threats facing a jurisdiction. Thus, analysis includes synthesizing data, developing inferences or conclusions, and making recommendations for action based on the data and inferences. These inferences constitute the finished intelligence product.

The process, along with investigative experience, also points out what has been done and what operational steps need to be taken. Thus, potential areas for further investigation may be recommended.[15] It is important to remember that the analyst *recommends* but does not direct or decide on policy alternatives to minimize crime problems.[16]

In 2004, a broad range of analytic techniques and methods were available to support law enforcement:

- **Crime analysis:** Crime pattern analysis, geographic analysis, time-series analysis, frequency-distribution analysis, behavioral analysis, and statistical analysis.
- **Investigative (evidential) analysis:** Network analysis; telephone record analysis; event, commodity, and activity-flow analysis; timeline analysis; visual investigative analysis; bank record analysis; net worth analysis; business record analysis; content analysis; postseizure analysis; case analysis; and conversation analysis.
- **Strategic analysis:** Threat assessments, premonitories, vulnerability assessments, risk assessments, estimates, general assessments, warnings, problem profiles, target profiles, and strategic targeting.

Analysis is quite simply a process of deriving meaning from data.

Dissemination

Dissemination requires getting intelligence to those who have the need and the right to use it in whatever form is deemed most appropriate. Intelligence reports kept within the intelligence unit fail to fulfill their mission.[17] Those who need the information are most often outside the intelligence unit; therefore, the current dissemination protocol is to share by rule and to withhold by exception.

Reevaluation

Reevaluation is the task of examining intelligence products to determine their effectiveness. Part of this assessment comes from the consumers of intelligence; that is, the managers, investigators, and officers to whom the intelligence is directed.

One way to reevaluate intelligence is to include a feedback form with each product that is disseminated.[18] To make sure the comments are valuable, the feedback form should ask specific questions relating to the usefulness of the intelligence.

Where We Stand Today

Several current strategies and philosophies in law enforcement have a direct bearing on intelligence-led policing.

Intelligence-Led Policing

The term "intelligence-led policing" originated in Great Britain. The Kent Constabulary developed the concept in response to sharp increases in property-related offenses (e.g., burglary and automobile theft) at a time when police budgets were being cut. Officials believed that a relatively small number of people were responsible for a comparatively large percentage of crimes. They believed that police officers would have the best effect on crime by focusing on the most prevalent offenses occurring in their jurisdiction.[19]

The Kent Policing Model, as it was originally called, de-emphasized responses to service calls by prioritizing calls and referring less serious calls for general nonpolice services to other agencies. Thus, more police time was available to create intelligence units to focus, initially, on property-related offenses in each of the jurisdiction's nine service areas. The result was a 24-percent drop in crime over 3 years.[20]

Intelligence-led policing focuses on key criminal activities. Once crime problems are identified and quantified through intelligence assessments, key criminals can be targeted for investigation and prosecution. Because the groups and individuals targeted in Kent were those responsible for significant criminal activity, the ultimate reduction in crime was considerable. The constabulary noted that "It has given the Kent Constabulary the ability to confront crime in an active, rational fashion and to build continually on each success."[21]

Intelligence-led policing in the United States has benefited from the recent development of "fusion centers," which serve multiagency policing needs. These fusion centers—derived from the watch centers of old—provide information to patrol officers, detectives, management, and other participating personnel and agencies on specific criminals, crime groups, and criminal activities. For example, they may support anti-terrorism and other crime-specific objectives. The centers may search numerous public and private databases to gather and analyze information. They may also generate intelligence products of their own, providing overviews of terrorist or other crime groups, analysis of trends, and other items of information for dissemination to participating agencies.

Since 2003, fusion centers have been established in many states. Currently, there are fusion centers in at least 25 states with more under development or being planned. The Iowa Fusion Center is part of that state's Law Enforcement Terrorism Prevention Program and a product of its State Homeland Security Strategy. The center serves as a clearinghouse for all potentially relevant, domestically generated homeland security data and information, leading to proper interpretation, assessment, and preventive actions.[22] It has several objectives, including providing a center for statewide strategic intelligence, centralized information management systems, regional operations support, and a 24-hour, 7-day-a-week watch center. It also supports multiagency information exchange and assigns an intelligence officer to each region.[23]

Funding for fusion centers is available through federal and state sources. As such, a center's mission can be limited to anti-terrorism, but many times includes all significant crimes, or targets different types of crime, such as identity theft, insurance fraud, money laundering, cigarette smuggling, armed robbery, and document fraud. The "all crimes" approach has recently been endorsed and recommended by many criminal intelligence advisory and policy groups.

Good policing is good terrorism prevention. In other words, professional policing of any kind is instrumental in uncovering intelligence associated with both terrorist activities and conventional crimes. Encouraging this perspective enables local police departments to involve line officers more actively and to reinforce the

fact that enforcement, crime prevention, and terrorism prevention are interrelated. This approach helps to balance the current emphasis on anti-terrorism activities with traditional anticrime efforts. Many line officers want to define their role in the fight against terrorism. Intelligence-led policing can help clarify their contributions in this regard.

Good policing is good terrorism prevention.

National Intelligence Model—United Kingdom

The United Kingdom's National Intelligence Model (NIM) considers the desired outcomes of an intelligence function to be community safety, crime reduction, criminal control, and disorder control.[24] To achieve these results, the model outlines the following objectives:

- Establish a task and coordination process.
- Develop core intelligence products to drive the operation.
- Develop rules for best training practices at all levels of policing.
- Develop systems and protocols to facilitate intelligence.[25]

Regular meetings keep participants focused on the stated goals and sustain the intelligence cycle.

Following are a few examples of how this model concept might function when adapted to U.S. circumstances:

- A county sheriff's office identifies narcotics control as its top priority and develops strategies accordingly. The office targets known offenders and groups, shuts down open-air drug markets and crackhouses, and participates in school-based drug awareness programs to help prevent drug use.
- A statewide agency identifies vehicle insurance fraud as a top area for enforcement. The agency targets those involved in staged accidents, identifies communities in which insurance fraud is prevalent, looks for similar methods of operation that may indicate ongoing fraudulent activity, and mounts a public education campaign.
- A police agency in a small city makes safe streets a priority. The agency focuses on directed enforcement in identified hotspots. It also targets career criminals whose apprehension will significantly reduce the number of crimes being committed. Preventive measures include enhanced patrols, improved street lighting, and crime watch programs.[26]

Each of these examples shows how prioritizing a particular criminal activity helps identify appropriate response strategies. Some of these responses are enforcement solutions, while others are environmental, educational, or community-oriented solutions.

Problem-Oriented Policing

Problem-oriented policing (POP) is a policing philosophy developed by Herman Goldstein.[27] As originally conceived, problem-oriented policing views crime control as a study of problems that leads to successful enforcement and corrective strategies. The model contends that "analysis, study, and evaluation are at the core of problem-oriented policing."[28]

POP requires assessing each new problem and developing a tailored response. This approach requires ongoing creativity, not simply finding one good idea and applying it unilaterally.

The SARA (Scanning, Analyzing, Responding, and Assessing) model is sometimes considered to be synonymous with problem-oriented policing, but it is a broader analytic model used in many fields. Nonetheless, the SARA model can be applied to collecting and applying intelligence. Scanning may be viewed as part of the collection process. Analysis and assessment are part of the intelligence process, and response is the outcome of the intelligence process.

Blending Intelligence and Problem-Oriented Policing

As noted earlier, intelligence operations are compatible with problem-oriented policing. Although the problem-oriented policing and SARA models align with intelligence processes, the intelligence aspects associated with problem-oriented policing often have been ignored.

Both community-oriented policing (COP) and problem-oriented policing have been used for crime analysis, which is statistical and incident-based, rather than strategic intelligence analysis, which looks at large-scope problems or models. Intelligence is a formal process of taking information and turning it into knowledge while ensuring that the information is collected, stored, and disseminated appropriately. Crime analysis data, usually collected for investigative purposes, typically does not meet the same standards as intelligence data—even though inferences may be drawn and recommendations may be made based on crime data. Confusion about the distinction between crime analysis data and intelligence data interferes with proper analysis and data handling in the police environment.

However, intelligence efforts do not always apply the first step in SARA (i.e., "Scan") and may benefit from developing more robust scanning mechanisms. At this point in the process, intelligence meets with standard patrolling and community-oriented policing because scanning occurs on the street. Research suggests that problem-solving analysts should "embrace both SARA and NIM" in the United Kingdom and show how the two merge.[29] Incorporating POP and SARA into intelligence-led policing is an excellent recommendation for U.S. agencies as well.

The U.S. model for intelligence-led policing incorporates the intelligence capabilities of all agencies. Traditionally, municipal agencies have relied on crime analysts, whereas agencies at the regional, state, and federal levels have used intelligence analysts. However, keeping crime analysis and intelligence analysis separate is not necessary. Agencies that can afford only one or two analysts must use professionals who can perform all types of analyses, not just statistical, network, or financial analyses.

Now is the time to eradicate the artificial barriers between local and regional-state-federal analysts. Analysts need to become familiar with a range of sources and techniques, rather than specializing in niche areas such as burglaries, gangs, or organized crime. Although some agencies may assign analysts to particular tasks, agencies will be best served by analysts who can perform all intelligence tasks regarding past, current, and potential crimes. This flexibility is made possible by a model that blends intelligence-led and problem-oriented policing.

This kind of intelligence blending also needs to take place at the beat level. Patrol officers are the eyes and ears of the police effort, and they must be encouraged and trained to look and listen intelligently. Information from field interviews, interactions with business people, and other activities and observations must be captured and forwarded to intelligence staff members who can analyze the data, arrive at appropriate courses of action, and send information back to the beat officers. The common practice of hoarding information or sharing it only with patrol officers should not continue; everyone with a need to know should receive intelligence results. For example, when intelligence officers are made aware of suspicious activities, they can analyze the information and provide officers on the street with pertinent guidance regarding officer safety and crime trends.

Patrol officers are the eyes and ears of the law enforcement effort, and they must be encouraged and trained to look and listen intelligently.

Police-Community Partnerships

COP has been an accepted policing strategy in the United States for the past decade. The tenets of COP include the following:

- Community policing partnerships.
- Crime prevention.
- Problem solving.

The fight against terrorism calls for locating and measuring terrorist risks to prevent terrorist actions, and local police have been enlisted in these efforts. How do local police determine potential threats in a given jurisdiction? They must know the community—i.e., its makeup, its ties to other countries or particular belief structures, and its potential for containing extremist or terrorist group members.[30] Police officers are particularly familiar with a community and its norms. For example, while on patrol, officers get to know who among community members associates with whom; they have firsthand knowledge of people's work and leisure habits.

Goldstein recognized the need to make greater use of rank-and-file police officers.[31] He believed that rank-and-file officers should be given greater latitude to think and be creative in their daily work and that

management should tap their accumulated knowledge and expertise, enabling officers to be more satisfied with their jobs and providing the citizenry with a higher return on their police investment.[32]

Empowering local officers with decisionmaking authority and making them aware of terrorist indicators may be key in preventing a terrorist attack.[33] Community- and problem-oriented policing support local awareness and involvement in solving crime problems. This involvement extends to anti-terrorism efforts. However, in the wake of the September 11 terrorist attacks, some agencies shifted officers from community policing to anti-terrorism efforts,[34] which may be counterproductive in helping to deter a terrorist attack.

Local law enforcement has been brought into the anti-terrorism fight and recognized for the role it plays. Alerts and information are being shared with local police more broadly than ever before. Methods for reporting suspicious activity to federal agencies have been created through regional and state links. Private citizens also have been included in the intelligence matrix through suspicious-activity tip lines, working groups with critical infrastructure managers, and other mechanisms to encourage reporting of unusual behavior that may be related to terrorism or other criminal activities.

These models illustrate that community- and problem-oriented policing are not at odds with policing against terrorism; instead, they are collaborative and complementary approaches.

Levels of Intelligence

For intelligence to work effectively, it must be a function that every department, regardless of size, can use. In general, law enforcement agencies can be categorized according to four levels of intelligence operations. The following categories are examples, not precise descriptors of any one agency's capabilities. Many variations in intelligence capabilities exist, and looking at an agency's size and resource capability is only one way of explaining those differences. For purposes of discussion, however, the following categories are used to identify a plan of action.

Level 1 intelligence is the highest level, the ideal intelligence-led policing scenario wherein agencies produce tactical and strategic intelligence products that benefit their own department as well as other law enforcement agencies. The law enforcement agency at this level employs an intelligence manager, intelligence officers, and professional intelligence analysts. Examples of level 1 intelligence agencies include the High Intensity Drug Trafficking Area (HIDTA) Intelligence Support Centers, the Financial Crimes Enforcement Network, and some state agencies that provide intelligence products, by request, to local law enforcement, such as the California Department of Justice, the Florida Department of Law Enforcement, the Arizona Department of Public Safety, and the Illinois State Police. Probably fewer than 300 agencies in the United States operate at level 1. These agencies may have hundreds or even thousands of sworn personnel.

The National Drug Intelligence Center is another example of a level 1 intelligence operation. NDIC, which has a higher ratio of analysts to sworn personnel than perhaps any U.S. agency, provides both tactical and strategic products in support of other agencies. It produces individual drug threat assessments for each state and a national drug threat assessment. It also uses "flying teams" of analysts who provide exploitation and postseizure analysis of documentation collected during investigations by other agencies. It does not, however, have an investigative mission of its own, as state and federal police agencies do.

Level 2 intelligence includes police agencies that produce tactical and strategic intelligence for internal consumption. In other words, these agencies generally use intelligence to support investigations rather than to direct operations. Such agencies may have a computerized database that is accessible to other departments, but they typically do not assign personnel to provide significant intelligence products to other agencies. These departments may have intelligence units and intelligence officers, analysts, and an intelligence manager. Some examples of level 2 intelligence agencies are state police agencies, large city police departments, and some investigating commissions. Agencies at this level may have hundreds to thousands of sworn personnel. Probably fewer than 500 agencies in the United States operate at this level.

An example of this type of agency might be a state-level law enforcement agency with police and/or prosecutorial powers. Such agencies use intelligence

analysis to support investigations into complex crimes such as organized crime, insurance fraud, and environmental crime. From time to time, this type of agency might produce a threat assessment or other strategic product to help guide its efforts. Most of its investigations are conducted independently, although the agency may sometimes join task force operations.

Level 3 intelligence is the most common level of intelligence function in the United States. It includes law enforcement agencies with anywhere from dozens to hundreds of sworn employees. These agencies may be capable of developing intelligence products internally, but they are more likely to rely on products developed by partner agencies, such as RISS centers, HIDTAs, federal intelligence centers, and state agencies. Some level 3 agencies may hire private intelligence analysts for complex cases. These types of departments do not normally employ analysts or intelligence managers, but they may have named one or more sworn individuals as their "intelligence officers" and may have sent them to intelligence and/or analytic training. Thousands of agencies nationwide are in this category. One authority notes that

> *while smaller agencies may not be able to devote a full-time position to the criminal intelligence function . . . [they] need to understand the proactive concept of criminal intelligence and recognize that most law enforcement agencies, regardless of size, are susceptible to organized criminal activity that may extend beyond jurisdictional boundaries. Their personnel should be trained to recognize and report indications of organized crime, gang activity, and criminal extremist and terrorist activity. The information should then be shared with intelligence-trained personnel from neighboring agencies. . . .*[35]

The same authority notes that "A viable option for . . . a medium-sized agency is to enter into a networking or mutual aid criminal intelligence agreement . . . with any number of surrounding law enforcement jurisdictions."[36]

Level 4 intelligence is the category that comprises most agencies in the United States. These agencies, often with a few dozen employees or less, do not employ intelligence personnel. If they assign someone to intelligence operations, that person generally has multiple responsibilities and is often a narcotics officer, gang officer, or counter-terrorism officer. Although some of these departments may be RISS members, most are involved in a limited information-sharing network made up of county or regional databases. Some departments have received intelligence awareness training and may be able to interpret analytic products.

Agencies that currently have no knowledge of or use for intelligence analysis should strive to achieve this basic intelligence capability. Such agencies can enhance their knowledge through online and other free training services. When properly trained, these agencies will be able to use any intelligence materials provided to them and to apply basic intelligence techniques to enhance their daily police operations.

Agencies that currently have no knowledge of or use for intelligence analysis should strive to achieve this basic intelligence capability.

A number of agencies may not fit strictly into one of these four categories. Some agencies may fall somewhere between level 3 and level 4, with a centralized database providing data support to numerous agencies but with no direct analytic support. Others may have analysts who support the mission of a specific bureau or section but who have no agencywide responsibility to provide products and direction. The key to intelligence-led policing is that sufficient interest and training should exist to create a culture of knowledge and intelligence in agencies nationwide.

What We Need To Do

Before an agency can develop intelligence-led policing, it must address several critical areas. Among these areas are the following:

- Blending intelligence and POP.
- Building stronger police-community partnerships.
- Blending strategic intelligence and police planning.
- Instituting information-sharing policies.
- Building analytic support for police agencies.

Basic Steps to Developing a Criminal Intelligence Capability

The resources that an agency needs to establish or renew intelligence operations depend on its existing capability and its managers' expectations.

Most guidance on this topic presumes that an agency can assign individuals to help develop the intelligence operation. One expert[37] suggests that agencies should follow the steps outlined below:

1. Create a proper environment, which includes obtaining the active support of the agency's chief executive officer, gaining political and budgetary support from the appropriate elected officials, and educating the agency and the community concerning the benefits of having a criminal intelligence function.
2. Establish the criminal intelligence unit as a proactive crime prevention operation that supports the concepts of community-oriented policing.
3. Design a unit mission statement focused on specific criminal activities and disseminate it to the entire agency.
4. Select qualified personnel, including a trained analyst, to staff the unit.
5. Obtain separate, secure quarters for the unit.
6. Implement and enforce professional guidelines for unit procedures, file procedures, security, special expense funds (confidential funds), and informant control.
7. Provide training for the chief executive officer, appropriate elected officials, criminal intelligence managers and supervisors, criminal intelligence officers and analysts, the remainder of the agency's personnel, and its legal advisor.
8. Liaison with neighboring agencies and participate in regional and state criminal intelligence networks. Join the Regional Information Sharing Systems and the Law Enforcement Intelligence Unit.
9. Require both strategic and tactical products from the unit and evaluate its operations on a regular schedule.
10. Ensure the chief executive officer meets regularly with the supervisor of the criminal intelligence unit to provide appropriate direction.

This model would be appropriate for level 1 and level 2 intelligence functions, but it is generally beyond the capabilities of levels 3 and 4.

In 2004, the Global Intelligence Working Group designed "10 Simple Steps to Help Your Agency Become Part of the *National Criminal Intelligence Sharing Plan*." This document helps agencies become more involved in intelligence sharing and provides useful advice, as shown in the excerpts below[38]:

1. Recognize your responsibilities and lead by example—implement or enhance your organization's intelligence function using the action steps in *NCISP*.
2. Establish a mission statement and a policy for developing and sharing information and intelligence within your agency.

3. Connect to your state criminal justice network and regional intelligence databases and participate in information sharing initiatives.

4. Ensure that privacy issues are protected by policy and practice. These can be addressed without hindering the intelligence process and will reduce your organization's liability concerns.

5. Access law enforcement web sites, subscribe to law enforcement listservs, and use the Internet as an information resource.

6. Provide your agency members with appropriate training on criminal intelligence.

7. Partner with public and private infrastructure sectors for the safety and security of the citizens in your community.

This checklist might serve those looking to establish a level 3 agency. Two steps that might be added are the following:

1. Designate one person, either an officer or a civilian analyst, as the agency contact for intelligence. Doing so will streamline training, information sharing, and intelligence interpretation functions (numbers 3, 5, and 6 above). Make certain that reports of suspicious activity from patrol officers and others are channeled to this individual.

2. Join a regional intelligence center or, if one is not available, work with other local agencies to form a regional center.

A level 4 agency might use the following steps, some taken from the lists above, to create its intelligence function:

1. Implement or enhance your organization's intelligence function using the steps shown.

2. Establish a mission statement and policies to address developing and sharing information and intelligence within your agency. Ensure that patrol officers' reports of suspicious activities are channeled to appropriate personnel.

3. Connect to your state criminal justice network and regional intelligence databases and participate in information sharing initiatives.

4. Ensure that privacy issues are protected by policy and practice. These can be addressed without hindering the intelligence process, and protecting privacy will reduce your organization's liability concerns.

These lists contain key concepts for implementing a successful intelligence operation. These concepts—i.e., developing a mission statement and policies, training, management and staffing, security, legal/privacy concerns, information sharing, and developing evaluation criteria—are described in more detail below.

Developing a Mission Statement and Policies

Regardless of the size and scope of its intelligence operations, every agency should have a mission statement and written policies that support those efforts. Policies can help define the support of command staff for intelligence-led policing and delineate department guidelines regarding intelligence operations.

> Policies enable the command staff to clearly define their support for intelligence-led policing and also delineate the guidelines the department will follow regarding any intelligence operations.

For agencies with an existing intelligence unit, a sample mission statement could be as follows:

> The _____ Department's Criminal Intelligence Unit will collect and analyze information on individuals and groups who are suspected of being involved in _____ and will provide this information to the chief executive officer for crime prevention and decisionmaking purposes.[39]

For agencies that do not have an intelligence unit (i.e., levels 3 and 4) but want to adopt an intelligence mission to support intelligence-led policing, the mission statement could be that given below:

> The _____ Department's intelligence mission is to actively participate in intelligence sharing initiatives by providing information and receiving intelligence products that will be used to enhance the department's ability to prevent and deter crime while abiding by legal constraints and being sensitive to the public's rights and privacy.

Like a well-written mission statement, intelligence policies and procedures may also curtail unwanted legal challenges to a department's authority (or may be the best defense against such legal challenges). Whereas policies outline an agency's requirements for and expectations of an intelligence operation, procedures delineate how those requirements should be implemented on a day-to-day basis.

Additional information to include in intelligence policies is contained in *Criminal Intelligence System Operating Policies* (28 C.F.R. Part 23) and the model intelligence policy developed by the International Association of Chiefs of Police National Law Enforcement Policy Center. The IACP model policy (see appendix D) is intended for agencies with intelligence units and for those with an intelligence function but no unit.

It should be noted that the IACP model policy discussion paper goes into greater detail on how an intelligence unit should function and is available from IACP. Several guidelines and standards have been adopted regarding criminal intelligence: 28 C.F.R. Part 23 and the Law Enforcement Intelligence Unit *Criminal Intelligence File Guidelines*. A copy of 28 C.F.R. Part 23 can be found on the Institute for Intergovernmental Research web site (www.iir.com); the LEIU guidelines are available at www.leiu-homepage.org/history/fileGuidelines.pdf.

Although 28 C.F.R. Part 23 is mandated only for those agencies receiving federal monies to fund intelligence systems (hardware or software), all agencies involved in intelligence operations will benefit from adopting these policies and the LEIU guidelines, as recommended by *NCISP.*

Training

Training is the key to change in any organization. The recent emphasis on intelligence reveals that many people involved in law enforcement, from commanders to patrol officers, do not fully understand the intelligence function and what it can accomplish. This misunderstanding is perhaps the greatest impediment to establishing intelligence-led policing. *NCISP* recommends that training be provided to all law enforcement personnel involved in criminal intelligence, and suggests that *NCISP* training standards be considered the minimum training standards.

Appendix D of *NCISP*[40] contains the "Core Criminal Intelligence Training Standards for United States Law Enforcement and Other Criminal Justice Agencies" (available at http://it.ojp.gov/documents/200507_ncisp.pdf). The standards call for training police executives, intelligence managers, intelligence officers, patrol officers, and analysts and includes a train-the-trainers module. It also includes training objectives for each level of training and notes a number of resources that may be tapped to support training.

For **law enforcement executives,** the *NCISP* core training standards recommend that a 4-hour block of training be provided within a police chiefs' association or another executive briefing environment. This training should focus on the philosophy of intelligence-led policing; legal, privacy, and ethical issues relating to criminal intelligence; existing information sharing networks and resources; and the intelligence process and the role it plays in supporting executive decisionmaking.

For **law enforcement officers,** the standards recommend a 2-hour block of training that could be provided during the recruits' basic training course or during inservice training. This block should focus on the officers' role in providing information to the intelligence process; the intelligence products that officers might obtain; available data systems, networks, and resources; and key signs of criminal activity.

For **intelligence commanders,** the standards recommend a 24-hour block of instruction in a classroom environment. The training should encompass training, evaluation, and assessment and effective criminal intelligence functions; personnel selection, ethics, policies and procedures, and intelligence products; intelligence-led policing and the criminal intelligence process; legal and privacy issues; tactical and strategic intelligence production; information sharing networks and resources; the development and implementation of collection plans; and practices for handling sensitive information, informant policies, and corruption prevention and recognition.

For **intelligence officers,** a 40-hour training session is recommended. This curriculum should address the intelligence process; legal, ethical, and privacy issues; resources found on the Internet and information sharing systems, networks, and other sources of information; proper handling of intelligence information, including file management and information

evaluation standards; processes for developing tactical and strategic intelligence products; the development of intelligence through critical thinking and inference analyses; and the development and implementation of information collection plans.

Analysts' training should also be 40 hours in length and should encompass the intelligence process; the importance of *NCISP;* proper handling of intelligence information; the analytic process; the development and implementation of collection and analytic plans; legal, privacy, and ethical issues relating to intelligence; research methods and sources; analytic methods and techniques; analytic skills; and computerized analytic tools.

NCISP core training standards also call for a train-the-trainer course for intelligence officers and intelligence commanders who will be training others. Such a course would be scheduled for 40 hours and would encompass the topics in the intelligence officers' and commanders' training courses, plus additional material on methods of instruction and adult learning.

Agencies that cannot designate personnel as intelligence officers or analysts may want to have officers with intelligence responsibilities trained in these techniques. A recent survey in New Jersey found that although fewer than 300 intelligence officers and analysts were assigned in the state, the requests for intelligence and analysis training totaled almost 900 seats.[41] Whatever level of intelligence an agency pursues, personnel involved in intelligence functions should have appropriate training. (Additional training resources are included in the appendixes.)

Management and Staffing

Successful intelligence operations depend on the responsibility and support of agency personnel. In a 28 C.F.R. Part 23 setting, the chief executive, or an appointee, is responsible for the intelligence operation.

According to *NCISP's* first recommendation regarding the management of intelligence operations, the chief executive officer and the manager of intelligence functions should do the following:

- 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 the management and supervision of the intelligence operation.
- Select qualified personnel for assignment to the intelligence operation.
- Ensure that standards are developed for background investigations of staff and system users to ensure that system facilities are secure and to protect access to the system or network.
- Ensure appropriate training for all personnel assigned to or affected 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 system for disseminating information appropriately.
- Implement a policies and procedures manual. The manual should establish agency accountability for the intelligence operation and should include policies and procedures regarding all aspects of the intelligence process.
- Promote a policy of openness when communicating with the public and other interested parties regarding the criminal intelligence process—that is, when doing so does not affect the security and integrity of the process.[42]

More than 30 years ago, the National Advisory Commission on Criminal Justice Standards and Goals supported the idea that any law enforcement agency with at least 75 sworn personnel should employ at least 1 full-time intelligence professional.[43] Best practices suggest having 1 intelligence analyst for every 75 sworn officers in generalized law enforcement agencies, with 1 for every 12 sworn officers in agencies with complex criminal investigative responsibilities, such as organized crime, narcotics, gangs, terrorism, and fraud.[44]

Opinions differ on who make the best analysts. Some agencies hire recent college graduates so the agencies can mold the new employees' training and experience.

Others use a combination of experienced and inexperienced analysts, pairing them so that the newer analysts learn from their colleagues. Others draw from the academic community on an occasional basis.[45] Another model, often used in Canada, is to use a mix of sworn officers and civilians. Promoting clerical support personnel with no research ability or experience into analytic positions is discouraged.

In most environments, significant pay inequities exist between the salaries of investigative and analytic staff. This disparity is changing slowly; however, as long as it exists, analysts will find other, more lucrative jobs after a few years in the law enforcement field. The International Association of Law Enforcement Intelligence Analysts recommends that analysts with the same number of years of experience as investigators receive similar pay.[46]

Security

Intelligence operations involve several levels of security: physical, programmatic, personnel-related, and procedural. Security is paramount for intelligence operations because the materials found in intelligence files may be unproved allegations rather than facts. Protecting the public and the agency's operations requires keeping information secure.

Security is paramount for intelligence operations because the materials found in intelligence files may be unproved allegations rather than facts.

Proper security restricts unauthorized access to information, protects information circulated within the department, and encourages the flow of data from the rest of the agency to the intelligence unit.[47] Physical security should reflect strict adherence to the safekeeping of files, computer access, and the office.[48] Visitors' logs should be kept for nonunit members entering the intelligence unit. The building and its internal spaces should have adequate security features. Computer equipment should be locked to prevent unauthorized access by nonintelligence personnel.

Programmatic security protects the computer hardware and software used for intelligence work. The most basic form of this type of protection is to password-protect computers so they cannot be operated by unauthorized personnel. Encrypting files and file transmissions is another level of programmatic security. Firewalls and virtual private networks provide additional security for information sharing.

Personnel security measures should include conducting background investigations of new employees, updating background investigations of current employees on a routine basis, and using polygraphs as necessary.[49] *NCISP* recommends that

> *. . . law enforcement agencies must conduct fingerprint-based background checks on individuals, both sworn and non-sworn, prior to allowing law enforcement access to the sensitive but unclassified communications capability. . . . [A]dditionally a name-based records check must be performed on law enforcement personnel every 3 years after the initial fingerprint-based records check is performed.*[50]

Policies and procedures also need to address security. According to 28 C.F.R. Part 23, administrative, technical, and physical safeguards must be adopted to prevent unauthorized access and intentional or unintentional damage (23.20[g]). It requires implementation of the following security measures:

- Adoption of effective and technologically advanced computer hardware and software designed to prevent unauthorized access.
- Restricted access to facilities, operating environments, and documents.
- Information storage such that information cannot be modified, destroyed, accessed, or purged without proper authorization.
- Procedures to protect criminal information from unauthorized access, theft, sabotage, fire, flood, or other natural or manmade disasters.
- Promulgation of rules and regulations to screen, reject from employment, transfer, or remove personnel who have direct access to the system (28 C.F.R. Part 23.20(g), 1–5).

Some best practices in security identified by the National White Collar Crime Center are found in *Secure Law Enforcement Computer Systems for Law Enforcement Executives and Managers.*[51]

Legal/Privacy Concerns

Respecting citizens' right to privacy and civil liberties is a primary concern when establishing or maintaining an intelligence operation. The activities of some

agencies in the 1970s and 1980s resulted in laws and regulations, primarily at the federal level, that support a lawful intelligence capability. However, few states have laws or guidelines concerning intelligence activities.[52]

The *Criminal Intelligence Systems Operating Policies* (28 C.F.R. 23.20) were created in the 1980s and were first applied to RISS centers. These regulations were then expanded to cover Organized Crime Narcotics projects and other database programs funded by the U.S. Department of Justice, Office of Justice Programs' Bureau of Justice Assistance. All criminal intelligence systems operating under the Omnibus Crime Control and Safe Streets Act of 1968, using federal funds, are required to conform with 28 C.F.R. Part 23, which protects the privacy and constitutional rights of individuals. (A copy of 28 C.F.R. Part 23 can be found at www.iir.com.)

NCISP recommends that all states voluntarily adopt 28 C.F.R. Part 23 to cover any intelligence system they use, regardless of federal funding. It also notes that agencies should use the LEIU *Intelligence File Guidelines* as a model for maintaining intelligence files. These two documents complement each other and endorse the same basic principles:

- Information entering the intelligence system should meet a criminal predicate or reasonable suspicion and should be evaluated to check the reliability of the source and the validity of the data.
- Information entering the intelligence system should not violate the privacy or civil liberties of its subjects.
- Information maintained in the intelligence system should be updated or purged every 5 years.
- Agencies should keep a dissemination trail of who received the information.
- Information from the intelligence system should be disseminated only to those personnel who have a right and a need to know in order to perform a law enforcement function.

Most states now have laws concerning the public's access to government records. Some states have an exemption in this law for intelligence and similar files. Some municipalities have laws that relate to collecting and maintaining intelligence files pertaining to individuals.

NCISP encourages law enforcement agencies involved in criminal intelligence sharing to use, when applicable, the policy guidelines provided in *Justice Information Privacy Guideline—Developing, Drafting and Assessing Privacy Policy for Justice Information Systems.*

Intelligence work must be conducted in an open manner, but doing so should not unreasonably conflict with the work itself. When the New Jersey State Police Department first developed intelligence policies in the 1970s, it provided the policies to the media and the public to demonstrate that the department was operating in an open manner in accordance with established agency policy. Such actions help to build community trust and police-community cooperation.

Intelligence work must be conducted in an open manner, but doing so should not unreasonably conflict with the work itself.

Information Sharing

Law enforcement agencies have focused on information collection during the past decade, but they have also increased their emphasis on information sharing. For example, the Bureau of Justice Assistance created a statewide intelligence systems program in 1993 to develop and facilitate statewide intelligence models[53] in compliance with 28 C.F.R. Part 23. Program grantees included the Tennessee Bureau of Investigation (which created the Automated Criminal Intelligence System of Tennessee), the Wisconsin Department of Justice (which created the Wisconsin Law Enforcement Intelligence Network), the North Dakota Office of the Attorney General (which created the North Dakota Law Enforcement Intelligence Network), the Connecticut State Police (which created the Statewide Police Intelligence Network), and the Utah Department of Public Safety (which enhanced the existing Utah Law Enforcement Intelligence Network).[54]

A 1998 monograph on statewide intelligence systems found that many state governments had established, or were in the process of establishing, statewide information systems. Forty-three state agencies either operated criminal intelligence databases or were planning to do so.[55]

From 1999 to 2000, IACP conducted a study that indicated that integrated information sharing systems are the most effective statewide systems.[56] The study included a review of justice system information sharing and onsite examinations in California, Colorado, Louisiana, Michigan, and North Carolina.

A 2003 survey by the Global Intelligence Working Group found 22 information sharing systems or initiatives in the United States, with RISS centers at the top of the list and a host of state and local systems nationwide. Other information sharing systems included CLEAR-Chicago, CISAnet (in southwest border states), JNET-Pennsylvania, MATRIX (Multistate Anti-Terrorism Information Exchange), SIN-Oklahoma, LEIU, ThreatNet-Florida, and HIDTAs.

Typically, these systems are hosted by a federal or large state agency and have up to several hundred agencies connected to them. Most of the systems surveyed included information on general crimes, terrorism, drugs, and gangs. In most systems, the data contributors retained ownership of the information.

A number of federal efforts are bringing together law enforcement in regional areas to combat crime. In the Houston area, for example, the Federal Bureau of Investigation (FBI) piloted a Field Intelligence Group (FIG) that is being used throughout the country. The Houston FIG's mission was to ensure that intelligence gathering and sharing functions within the Houston FBI were coordinated across investigative programs, with FIG serving as a one-stop shop for the analysis and processing of raw data gathered in the course of investigative activity. FIG created a multiagency clearinghouse for Super Bowl XXXVIII, in cooperation with a dozen agencies at the federal, state, and local levels, to ensure safety at that major event.

In May 2004, the U.S. Department of Justice (DOJ) shared draft copies of its Law Enforcement Information Sharing (LEIS) strategy with state and local law enforcement professionals. The LEIS strategy calls for:

- Law enforcement agencies throughout the country to access shareable DOJ information on a timely and secure basis.
- DOJ to provide its law enforcement partners with effective new capabilities and services for accessing, analyzing, and disseminating investigative and intelligence information.
- LEIS partners to share information with each other and to abide by strict guidelines to ensure accountability, security, and privacy.[57]

DOJ is continuing to work on implementing LEIS.

The Joint Terrorism Task Forces (JTTFs), headquartered in FBI offices nationwide, have also encouraged information sharing and cooperative efforts. For example, the JTTF in Houston created a Counter Terrorism Intelligence Group (CTIG) that has provided state and local agencies with indicators of suspicious activities. The CTIG provides a bulletin to local agencies containing the latest information on suspicious activities in the region. In 6 months, 173 agencies signed up to participate. By affirming that information sharing is a two-way street, the Houston CTIG increased its input of information from local agencies to the FBI by 50 percent. Today, the Houston CTIG provides training for other state and local law enforcement agencies.

Developing Evaluation Criteria

One reason why intelligence operations are not always understood or appreciated is because they cannot be evaluated by traditional measures of law enforcement success, such as the number of arrests and indictments attributable to law enforcement officers, units, or agencies. The inability of law enforcement administrators to evaluate intelligence has in some ways undermined its credibility.[58]

There are, however, concrete ways to evaluate intelligence. A monthly evaluation of intelligence operations might ask the following questions:

- Does the unit know more this month about organized crime activities in its jurisdiction than it did last month?
- What has been learned? How? Could more have been learned by better approaches? Can specific cases be developed? Should there be a shift in investigative efforts?
- Has information been provided from other agency personnel? Have the reports from patrol officers been dealt with appropriately?

- Has the filing system effectively handled the questions directed to it?
- Have the consumers been queried as to the usefulness and accuracy of the intelligence materials?[59]

Success Stories

Success stories in the areas of intelligence and analysis are not as numerous as one might hope. However, once agencies begin to use intelligence more fully, success stories should be easier to identify. Some examples of effective intelligence and analysis operations appear below.

Jefferson County, Colorado

In the early 1990s, the Jefferson County Sheriff's Office and the Lakewood Police Department combined their vice and intelligence units' functions to improve their resources. Part of this merger included access to each other's agency records and intelligence information. In 2001, the two agencies adopted the CrimNtel software program to help manage their intelligence information. This database complies with 28 C.F.R. Part 23 and supports the collection, maintenance, and dissemination of police intelligence records, including criminal information about gangs, criminal extremists, and vice and narcotics activities.

In 2003, the City of Arvada Police Department joined the Jefferson and Lakewood merger by connecting to CrimNtel. As of 2004, the Jefferson County Sheriff's Office Detentions Division was in the final stages of linking to the database, which will increase the amount of available data. Although the database was not completely regionalized, it gave these agencies access to some of the largest agency record pools in the Denver area, fostering cooperation and facilitating intelligence sharing.

Charlotte-Mecklenburg, North Carolina, Police Department

The Charlotte and Mecklenburg police departments joined forces in the 1990s (for a total of 1,501 combined officers in 2001). They then brought in Herman Goldstein, the "father of problem-oriented policing," to audit the department to see how consistently community-policing and problem-solving models were being applied. He and Ronald Clarke, of Rutgers University, worked with the police to create different approaches to crime in the area. They found that many officers quickly scanned a crime problem and then moved immediately to the response phase, bypassing any analysis of available data to determine the most appropriate response. Consequently, problems were not solved as effectively as they might have been.

Analyzing the data, Goldstein and Clarke concluded that four major crime problems were occurring in the area: appliance burglaries from single-family homes under construction, vehicle larceny in central city parking lots, drug-related violence in the Belmont community, and the possible connection of pawnshops to burglaries. On the basis of this intelligence, they then analyzed the circumstances surrounding each crime problem to develop appropriate action plans. Because each circumstance was different, differing strategies were used. In all cases, however, data analysis allowed them to identify strategies that reduced crime. (Information taken from "Advancing Community Policing" grantee site report, available at www.cops.usdoj.gov.)

Rockland County, New York

The Rockland County Intelligence Center (RCIC) was formed in 1995 in Rockland County to coordinate and disseminate intelligence information among law enforcement agencies. Representatives from seven local agencies participate in RCIC. The salaries of these representatives are reimbursed by the county; five county personnel are also employees. RCIC and its operations are governed by an oversight committee composed of county police chiefs and three municipal and two county representatives.

RCIC accesses several databases, including MAGLOCLEN (Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network, a RISS center), the Rockland County Police Information Network (which has nine agencies contributing to it), the New York City Construction Authority Mobnet database, the New York/New Jersey HIDTA database, the National Insurance Crime Bureau, Auto-Trak, New York State Parole, the Photo Imaging Network, and the New York Division of Criminal Justice Services Sex Offender Registry. RCIC also cooperates with UNYRIC (Upstate New York Regional Intelligence Center, managed by the New York State Police).

RCIC disseminates information bulletins on new crime trends or high-priority issues. It provides monthly

burglary/robbery analysis reports, gang awareness patterns, telephone toll analysis, and crime mapping.

Hayward, California, Police Department

Hayward is a municipality near San Francisco with a population of about 144,600. Its police department has almost 200 sworn officers.[60] After receiving a Department of Homeland Security grant, the Hayward Police Department created a full-time detective position focused specifically on homeland security issues. By contacting the Financial Investigations Program (FIP) of the California Department of Justice's Bureau of Narcotics Enforcement, the Hayward Police Department was able to access FinCEN data regarding suspicious financial transactions. The department requested reports on suspicious activity by ZIP Code and received 450 suspicious activity reports. An analysis of the reports revealed links to an outlaw motorcycle gang, possible organized crime groups, and terrorist financing.

As a result, the Hayward Police Department is conducting a joint investigation with the U.S. Bureau of Immigration and Customs into a subject with ties to terrorist financing and who has laundered more than $100 million during a 3-year period.

The Hayward Police Department also has been able to access investigative and analytic support from the U.S. Department of Justice's FIP, including access to a wide range of commercial databases. One outcome of this work is the improved relationship between the police department and its local financial institutions. The institutions now contact the police proactively about suspicious financial activity reports, cutting the lag time between when a suspicious activity occurs and when police learn about it.

As a result of this success in the financial investigative area, the Hayward Police Department now requests a FinCEN check on every subject who is investigated for possible terrorist connections.

New Jersey Department of Corrections

Few states have coordinated efforts between police and corrections to share information on gangs. Law enforcement intelligence suggests that gang leaders in prison delegate responsibility to members on the street, which allows gangs to prosper despite the incarceration of gang leaders. After several attacks on staff and inmates, the New Jersey Department of Corrections (NJDOC) began an initiative in 1997 to identify and monitor gang-affiliated inmates.

More than 8,000 gang members have been identified, and half of them are currently incarcerated. The NJDOC Intelligence Section has made managing gangs within the prison and disseminating gang-related intelligence to other departments a priority.

To keep abreast of changing gang activity codes and crimes, NJDOC reviews correspondence and other research containing information on gang organizations, structure, codes, affiliations, and membership. In addition to generic intelligence, several agencies with established gang identification databases help NJDOC identify the gang affiliation of incoming state prison inmates. This additional intelligence is one of several identification criteria used when an inmate arrives at intake.

Inmates must meet two of eight standard criteria to be classified as gang members (criteria include self-admission, group/gang photo, and correspondence from other gang members). NJDOC shares this information through four initiatives: the Inter-Institutional Intelligence Committee, identification lists, ad hoc inquiries, and the Gang Reduction and Aggressive Supervised Parole program.

Soon after NJDOC recognized the importance of gang identification and the sharing of intelligence, it developed the Inter-Institutional Intelligence Committee. This committee comprises investigators and detectives from multiple agencies throughout the state and meets once a month. Attendees include members from federal, state, regional, county, and local law enforcement agencies. A monthly bulletin, distributed to those in attendance, highlights new tattoos, codes, graffiti, statewide trends, identification statistics, recent news, and incident reviews.

To provide information throughout the state, gang identification lists are generated by geographic region. Ad hoc inquiries on gang members are also available. The fourth information sharing program (Gang Reduction and Aggressive Supervised Parole) focuses on paroled inmates. Every identified gang inmate on parole is assigned to a special caseload and monitored closely by a parole officer who understands gang issues. The program is a collaborative effort between NJDOC, the New Jersey State Police, and the New Jersey State Parole Board.

Iowa Law Enforcement Information Network

In 1984, Iowa law enforcement agencies joined to form the first state-level effort to regularly exchange information on suspected offenders. The Iowa Law Enforcement Intelligence Network (LEIN) consists of state and local law enforcement officers who complete a 2-week criminal intelligence course conducted by the Iowa Department of Public Safety (DPS). As of 2004, LEIN's membership consisted of about 730 officers from more than 200 agencies.

After attending the criminal intelligence course, intelligence officers gather information and forward it to the Iowa DPS Intelligence Bureau, where it is analyzed and disseminated back to LEIN members. A yearly conference updates the officers on new trends and activities in a range of criminal areas. A similar program has been implemented in Illinois, Kansas, Nebraska, North Dakota, South Dakota, and Wisconsin.

One example of LEIN's effectiveness is illustrated by a 1998 case in which LEIN members worked together to investigate a series of bank robberies occurring in the Iowa City area. Officers from six departments participated in a surveillance investigation that resulted in the bank robber's arrest. Another example, in 1999, involved seasonal, transient home repair workers who engaged in fraudulent criminal activity, particularly against senior citizens. The LEIN program conducted a 2-day training seminar and intelligence briefing on these activities in advance of the summer season, and fewer incidents of fraud were reported that year than in earlier years.[61]

In July 2002, the Iowa DPS cooperated with a number of local law enforcement agencies to conduct an undercover operation in the Des Moines metro area. Working out of a storefront, undercover officers contacted individuals who agreed to sell narcotics, stolen merchandise, and a significant number of stolen vehicles. These items included property taken from several burglaries in central Iowa. About 50 potential defendants were identified. Narcotics and stolen property with an estimated total value of $1.25 million, including more than 100 stolen vehicles, were seized or recovered.

Participating as LEIN members in this investigation, several agencies joined forces to resolve a large number of burglary, theft, fraud, and narcotics cases. Through this effort, officers identified, in a relatively short period, many individuals involved in multiple crimes.

Coventry, Connecticut, Police Department

Coventry, a rural town of 11,500 in northeastern Connecticut, has 13 sworn officers. The Coventry Police Department (CPD) believed that areas in the community with a high proportion of student rental properties accounted for a significant increase in crime and calls for service. However, CPD's paper-based reporting system made it difficult to retrieve and analyze information about suspects, victims, witnesses, and locations.

A Community-Oriented Policing Services grant helped CPD buy a computer-aided dispatch system and upgrade its records management system in 2002. The new system offered case management and crime analysis functions. The crime analysis data allowed CPD to see that domestic violence was one of the highest calls-for-service problems in the lakeside communities. It also revealed a burglary problem in the downtown area, so officers worked with businesses and residents to find a solution. The automated booking program saved officers considerable time. As a result of the updated technology, officers now have more effective tools with which to analyze and respond to neighborhood problems.[62]

Louisiana State Police

The analytical unit of the Louisiana State Police's investigative office includes a sergeant, 2 analyst chiefs, 12 analysts, and a clerk chief. The unit provides case support and tactical response on a daily basis.

Recently, the analytical unit worked with investigators from the Louisiana State Police Gaming Section on an illegal gambling case. The analysts read reports pertaining to the case and prior cases relevant to the subjects involved; completed background checks on all subjects, querying various databases and sources; analyzed subpoenaed telephone records; and prepared charts of associations, phone calls, and money transactions. The analysts reviewed evidence taken from the suspects' trash and helped collect evidence when the search warrant was served. As a result of this intelligence effort, seven people were arrested and case files were opened for several others.

Appendix A: Information Sharing and Information Technology Resources

International Association of Chiefs of Police
www.theiacp.org

The International Association of Chiefs of Police (IACP) supports police commanders regarding a range of issues, including intelligence. Its web site contains intelligence policies, information on training workshops, and publications (e.g., the 2002 *Criminal Intelligence Sharing Summit Report, A Police Chief's Primer on Information Sharing,* and *Leading from the Front: Combating and Preparing for Domestic Terrorism*). IACP has been involved in the Criminal Justice Information Sharing project with the Global Intelligence Working Group and the Institute for Intergovernmental Research. IACP provides training on topics of interest to the intelligence field, from organized crime and nontraditional organized crime to undercover operations, informant management, analysis, and principles of report writing.

International Association of Law Enforcement Intelligence Analysts, Inc.
www.ialeia.org

The International Association of Law Enforcement Intelligence Analysts, Inc. (IALEIA), an organization of analysts, intelligence officers, and police managers, was founded in 1980. It has about 1,800 members in more than 50 countries. A nonprofit organization dedicated to educating the police community about the benefits of intelligence and analysis, IALEIA trains analysts to meet high standards of professionalism.

In the past decade, it has published a number of documents relating to intelligence and analysis, including the following:

- *Successful Law Enforcement Using Analytic Methods.*
- *Guidelines for Starting an Analytic Unit.*
- *Intelligence Models and Best Practices.*
- *Intelligence-Led Policing.*
- *Starting an Analytic Unit for Intelligence-Led Policing.*
- *IALEIA Journal 20th Anniversary CD–ROM.*
- *Intelligence 2000: Revising the Basic Elements* (produced jointly with the Law Enforcement Intelligence Unit (LEIU).
- *Turnkey Intelligence: Unlocking Your Agency's Intelligence Capability* (a CD–ROM produced jointly with LEIU and the National White Collar Crime Center).

IALEIA participated in the development of the Foundations of Intelligence Analysis Training program (with LEIU, RISS centers, and the National White Collar Crime Center) and offers the course, which is taught by experienced analytic instructors. The IALEIA web site lists available training and reference materials.

Office of Community Oriented Policing Services
www.cops.usdoj.gov

The Office of Community Oriented Policing Services (COPS) offers a range of publications and tools to assist with problem-oriented policing and analysis. Its web site has a problem-oriented policing center (www.popcenter.org) with publications including *Using Analysis for Problem Solving,* "Assessing Responses to Problems: An Introductory Guide for Police Problem Solvers," and other reports and articles, some of which are reprinted from other sources.

COPS also offers documents on intelligence sharing that include the two listed below:

"Connecting the Dots for a Proactive Approach" (www.cops.usdoj.gov/mime/open.pdf?Item=1046) Community policing is an important part of preparing for and responding to acts of terrorism. This article in *Border and Transportation Security* magazine details the work of three COPS staffers who harness the power of community policing to enhance homeland security.

Protecting Your Community From Terrorism: Strategies for Local Law Enforcement, Volume 4: The Production and Sharing of Intelligence
(www.cops.usdoj.gov/mime/open.pdf?Item=1438)
This document discusses the importance of intelligence-led policing and its correlation with problem-oriented policing principles. The report outlines criteria for an effective intelligence function at all levels of government. Sidebars highlight contributions from key players in the fields of intelligence and policing.

U.S. Department of Justice—Office of Justice Programs
www.ojp.usdoj.gov

The U.S. Department of Justice (DOJ) Office of Justice Programs (OJP) has initiated several programs regarding information technology and information sharing through its bureaus and offices including the Bureau of Justice Assistance, National Institute of Justice, and Bureau of Justice Statistics.

OJP's Information Technology web site (www.it.ojp.gov) provides a wealth of information on a variety of programs and initiatives, including online tools that support information sharing at all levels of government, and the recommendations of DOJ's Global Justice Information Sharing Initiative.

The web site also provides information on:

- Justice Standards Clearinghouse for Information Sharing.
- DOJ's Global Justice XML Data Model (GJXDM).
- National Information Exchange Model (NIEM), a partnership between DOJ and DHS.
- Privacy policies and public access.
- *National Criminal Intelligence Sharing Plan.*
- An information technology and information sharing event calendar and a document library.

Regional Information Sharing Systems
www.rissinfo.com

The Regional Information Sharing Systems (RISS) comprise six regional intelligence centers operating in mutually exclusive geographic regions. It provides criminal information exchange, secure communications, and other related services to local, state, tribal, and federal law enforcement member agencies. RISS disseminates critical information for investigative support in combating multijurisdictional crime that requires interagency cooperation.

RISS is a federally funded program administered by the U.S. Department of Justice Office of Justice Programs' Bureau of Justice Assistance. Information retained in RISS criminal intelligence databases must also comply with the *Criminal Intelligence Systems Operating Policies* (28 C.F.R. Part 23).

The executive director and policy board chairperson of each center constitute the RISS Directors National Policy Group, which has direct control over the policies and operations of the secure, nationwide law enforcement communications and information sharing network (RISSNET) and related resources.

RISS membership has grown to serve more than 7,100 law enforcement and criminal justice agencies representing more than 700,000 sworn officers. Membership includes local, state, federal, and tribal law enforcement member agencies in all 50 states, the District of Columbia, U.S. territories, Australia, Canada, and England. Agencies must join their regional RISS center through an application process established by the center.

RISS history includes many achievements and successes in helping member agencies share information and combat multijurisdictional crime problems. A few milestones are mentioned below.

In 1997, RISS implemented RISSNET. Today, this network allows member agencies to access many resources electronically. RISSNET features include online access to a RISS bulletin board, databases, RISS web pages, secure e-mail, and a RISS search engine. To use the network, officers of member agencies must obtain a security package and enroll in RISSNET. The more than 7,100 law enforcement member agencies all have access to RISSNET nationwide.

During 1999, RISS began expanding RISSNET to link to state and federal law enforcement agency systems and provide additional resources to all users. As of

April 2004, 16 High Intensity Drug Trafficking Areas, 15 state agencies, and 8 other federal and regional systems were connected to RISSNET.

In September 2002, the Federal Bureau of Investigation (FBI) Law Enforcement Online (LEO) system was connected with RISS. In October 2003, the RISS/LEO interconnection was recommended in the *National Criminal Intelligence Sharing Plan (NCISP)* as the initial sensitive but unclassified communications backbone for implementing a nationwide criminal intelligence sharing capability. *NCISP* encourages agencies to connect their system to RISS/LEO.

In April 2003, RISS expanded its services and implemented the Automated Trusted Information Exchange (ATIX) to provide additional users with access to information on homeland security, disaster response, and terrorist threats. RISS member agencies and officials from first responder agencies and critical infrastructure entities can access ATIX.

Contact information for each RISS center is as follows.

MAGLOCLEN
Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network
140 Terry Road, Suite 100
Newtown, PA 18940
www.info@magloclen.riss.net

MOCIC
Mid-States Organized Crime Information Center
1610 East Sunshine Drive, Suite 100
Springfield, MO 65804
www.info@mocic.riss.net

NESPIN
New England State Police Information Network
Grove Street, Suite 305
Franklin, MA 02038
www.info@nespin.riss.net

RMIN
Rocky Mountain Information Network
2828 North Central Avenue, Suite 1000
Phoenix, AZ 85004
www.info@rmin.riss.net

ROCIC
Regional Organized Crime Information Center
545 Marriott Drive, Suite 850
Nashville, TN 37214
www.info@rocic.riss.net

WSIN
Western States Information Network
1825 Bell Street, Suite 205
Sacramento, CA 92403
www.info@wisn.riss.net

U.S. Drug Enforcement Administration
www.dea.gov

The U.S. Drug Enforcement Administration (DEA) has several programs to assist state and local law enforcement intelligence efforts. One of these is the National Drug Pointer Index (NDPIX).

In 1992, DEA was designated by the Office of National Drug Control Policy to develop a national drug pointer system to help federal, state, and local law enforcement agencies investigate drug trafficking organizations and to enhance officer safety by preventing duplicate investigations. The DEA recognized that the development of this system would require a cooperative effort among state, local, and federal law enforcement agencies.

The DEA drew from the experience of state and local agencies to make certain that their concerns were addressed and that they had extensive input and involvement in the development of the system. Nominees from 19 states and 24 law enforcement organizations formed a project steering committee and 6 working groups.

NDPIX became operational nationwide in October 1997. The National Law Enforcement Telecommunications System—a familiar, fast, and effective network that connects to almost every police entity in the United States—is the backbone for NDPIX. Participating agencies are required to submit active case targeting information to NDPIX to receive pointer information. The greater the number of data elements entered, the greater the likelihood of identifying possible matches. Designed to be a true pointer system rather than an intelligence system, NDPIX serves as a switchboard that provides timely

notification of common investigative targets. The actual case information is shared only when telephonic contact is made between the officers and agents who have been linked to NDPIX by their agencies. DEA is a full participant in NDPIX and had entered 86,000 drug investigative targets into the system as of June 2000. As more and more law enforcement agencies participate in NDPIX, the system will provide far-reaching assistance in the effort to dismantle drug organizations.

The publications section of the DEA web site (www.dea.gov/pubs/publications.html) provides dozens of reports in a downloadable format. The intelligence section has both country profiles and drug reports. Recent country profiles include reports on Australia, Belize, China, and India. Recent drug reports include the following:

- *Heroin Signature Program: 2001.*
- *2002 Domestic Monitor Program.*
- *Heroin Trafficking in Russia's Troubled East.*
- *Drug Trade in the Caribbean: Threat Assessment.*

Appendix B: Sources of Intelligence Products

Bureau of Alcohol, Tobacco, Firearms and Explosives
www.atf.gov

Now a part of the U.S. Department of Justice, the Bureau of Alcohol, Tobacco, Firearms and Explosives produces intelligence publications on arsons and explosives. Two such publications include the *Bomb Threat Checklist* and *2000 Threat Assessment Guide for Houses of Worship.*

California Department of Justice
www.caag.state.ca.us

The California Department of Justice publishes intelligence bulletins, alerts, and reports on gangs, organized crime, and other topics. Some, such as *Organized Crime in California 2003,* are available on its web site; others are available only through a secure intranet.

El Paso Intelligence Center
www.dea.gov/programs/epic.htm

The El Paso Intelligence Center (EPIC) was formed in 1974 to establish a Southwest Border Intelligence Service Center staffed by representatives from the DEA, Immigration and Naturalization Service (INS), and U.S. Customs Service (U.S. Department of the Treasury). The director is a representative from the U.S. Drug Enforcement Administration (DEA), and the deputy director is from INS.

A number of EPIC programs are dedicated to postseizure analysis and establishing links between recent enforcement actions and ongoing investigations. EPIC personnel coordinate and conduct training seminars throughout the United States, covering topics such as indicators of trafficking and concealment methods used by couriers. Through its Operation Pipeline program, EPIC trains state and local officers in highway drug and drug currency interdiction.

In a continuing effort to stay abreast of changing trends, EPIC developed the National Clandestine Laboratory Seizure Database. EPIC's future course will be driven by the National General Counterdrug Intelligence Plan. As a major national center in the new drug intelligence architecture, EPIC will serve as a clearinghouse for the High Intensity Drug Trafficking Areas (HIDTA) Intelligence Centers, gathering state and local law enforcement drug information and providing drug intelligence to the centers.

EPIC includes 15 federal agencies, and it has established information sharing agreements with law enforcement agencies from all 50 states, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, and Canada.

Federal Bureau of Investigation
www.fbi.gov

Online Federal Bureau of Investigation (FBI) publications include current and back issues of the *FBI Law Enforcement Bulletin* and a number of reports. *Terrorism in the United States* is available for 1996, 1997, 1998, and 1999. *Countering Terrorism: Integration of Practice and Theory* is available in a downloadable format, as is *CONPLAN: U.S. Government Interagency Domestic Terrorism Concept of Operations.* Another publication, *The School Shooter: A Threat Assessment Perspective,* can also be found on the FBI web site. This web site also provides information on the National Law Enforcement Data Exchange (N–DEx), the Regional Data Exchange (R–DEx), and Sentinel.

Federation of American Scientists—Intelligence Research Program
www.fas.org/irp/crs

This web site provides intelligence-related documents published by the Congressional Research Service,

including many studies on intelligence efforts and terrorist groups.

Financial Crimes Enforcement Network
www.ustreas.gov/fincen

The Financial Crimes Enforcement Network (FinCEN) was established in April 1990. Its original mission was to provide a governmentwide, multisource intelligence and analytical network to support the detection, investigation, and prosecution of domestic and international money laundering and other financial crimes. In 1994, its mission was broadened to include regulatory responsibilities.

FinCEN's current mission is to support law enforcement investigative efforts, foster interagency and global cooperation against domestic and international financial crimes, and provide U.S. policymakers with strategic analysis of domestic and worldwide money laundering developments, trends, and patterns. FinCEN achieves this mission by collecting and analyzing information, providing technological assistance, and implementing U.S. Treasury regulations.

FinCEN controls more than 170 million reports filed under the Bank Secrecy Act and other similar laws. These reports are accessed by federal, state, and local law enforcement agencies through the Gateway Program.

FinCEN's web site offers a number of open-source publications relating to financial intelligence, including monographs on terrorist financing through informal value transfer systems, trend reports, and other publications. The site also links to publications produced by the Financial Action Task Force and lists money service businesses registered in the United States by state.

Florida Department of Law Enforcement
www.fdle.state.fl.us

The Florida Department of Law Enforcement publishes a number of online informational reports and studies on topics such as check fraud, identity theft, narcotics, voter fraud, and Internet safety.

High Intensity Drug Trafficking Areas
www.whitehousedrugpolicy.gov/hidta

The Anti-Drug Abuse Act of 1988 authorized the Director of the Office of National Drug Control Policy (ONDCP) to designate areas within the United States that exhibit serious drug trafficking problems and harmfully affect other areas of the country as High Intensity Drug Trafficking Areas (HIDTAs). The HIDTA program provides federal funds to those areas to help eliminate or reduce drug trafficking and its harmful consequences. Since 1990, 31 areas have been designated as HIDTAs.

The HIDTA program facilitates cooperation between drug control organizations by providing them with resources and information and by helping them reorganize and pool resources, coordinate and focus efforts, and implement joint initiatives. The key priorities of the program are as follows:

- Assessing regional drug threats.
- Designing strategies that focus on combating drug trafficking threats.
- Developing and funding initiatives to implement strategies.
- Facilitating coordination between federal, state, and local efforts.
- Improving the effectiveness and efficiency of drug control efforts to reduce or eliminate the harmful impact of drug trafficking.

The HIDTA program has 31 regional offices operating in 40 states. Each HIDTA is governed by its own executive committee composed of approximately 16 members—8 federal members and 8 state or local members. These committees ensure that threat-specific strategies and initiatives are developed, employed, supported, and evaluated.

HIDTA Intelligence Service Centers have been mandated to facilitate the timely exchange of information among participating agencies. They also were tasked with the following:

- Establishing event and case deconfliction systems, where needed.
- Developing drug threat assessments for HIDTA areas of responsibility.
- Conducting postseizure analysis of major drug seizures related to HIDTA.
- Assisting state and local agencies in reporting drug seizures to the El Paso Intelligence Center.
- Participating in online intelligence reporting systems.
- Providing photo-imaging network capability in concert with NCIC 2000 and the Integrated Automated Fingerprint Identification System.[63]

The HIDTA program established Investigative Support Centers (ISCs) in designated areas to facilitate information sharing, intelligence collection, analysis, and dissemination. ISCs also provide technical and strategic support to HIDTA initiatives and participating agencies. A state or local law enforcement agency and a federal law enforcement agency jointly manage ISCs. The multiagency personnel at ISCs provide event and subject deconfliction services for HIDTA task forces and other law enforcement agencies inside and outside the HIDTA region for increased officer safety. They also provide intelligence to increase the effectiveness and efficiency of task forces by analyzing information and identifying drug trafficking organizations and their vulnerabilities. HIDTA ISCs provide secure sites and information systems that participating law enforcement agencies can use to store and appropriately share information and intelligence.

Each HIDTA produces an annual drug threat assessment, which is created with information received from regional drug control agencies. The threat assessments identify the regional drug threat to help departments and agencies develop strategies and learn about intelligence gaps. The assessments also help policymakers determine drug threat priorities and resource allocations. HIDTA drug threat assessments are integrated and coordinated with the National Drug Intelligence Center (NDIC), which is responsible for producing the national drug threat assessment.

The National HIDTA Assistance Center at www.nhac.org is an overall HIDTA assistance center in Miami that provides training and other resources to HIDTA participants.

Law Enforcement Intelligence Unit
www.leiu.org

On March 29, 1956, representatives from 26 law enforcement agencies met in San Francisco and formed the Law Enforcement Intelligence Unit (LEIU). LEIU records and exchanges confidential criminal information that is not available through regular police communication channels.

LEIU has performed a valuable coordinating function among law enforcement agencies throughout the United States, Canada, and Australia. Its membership is divided geographically into four zones: the Eastern Zone, Central Zone, Northwestern Zone, and Southwestern Zone. Each zone has a chairperson and a vice chairperson. The governing body of LEIU is the executive board, which establishes policy and oversees the admission of law enforcement agencies applying for membership. The board is composed of national officers, zone officers, the past general chairperson, a legal adviser, and a representative from the California Department of Justice (which is the Central Coordinating Agency for LEIU).

LEIU membership is open to state and local law enforcement agencies that have a criminal intelligence function. Applicants must be sponsored by a current member. LEIU has approximately 250 members.

LEIU holds one annual training conference on general matters and one on gaming issues. It has a central repository pointer index that its members can query confidentially. LEIU produces publications on intelligence issues of interest to its members. It also offers a gaming index containing the names and identifiers of individuals applying for gaming licenses. An analyst is available to respond to members' inquiries for information on suspected criminals and their activities.

LEIU may be reached at the California Department of Justice, Bureau of Investigation, Intelligence Operations Program, Central Coordinating Agency, P.O. Box 163029, Sacramento, CA 95816–3029.

Library of Congress—Federal Research Division
www.loc.gov/rr/frd/terrorism.html

This division of the Library of Congress houses a Terrorism and Crime Studies section with bibliographies on particular topics and numerous reports covering subjects such as terrorism, organized crime, narcotics distribution, and transnational organized crime.

National Drug Intelligence Center
www.usdoj.gov/ndic

The National Drug Intelligence Center (NDIC) supports national policy and law enforcement decisionmakers by providing timely, strategic assessments focusing on the production, trafficking, and consumption trends and patterns of illicit drugs inside U.S. national borders and territories.

The *National Drug Threat Assessment,* NDIC's major intelligence product, is a comprehensive annual report on national drug trafficking and abuse trends within the United States. The assessment identifies the primary drug threat to the nation, monitors fluctuations in consumption levels, tracks drug availability by geographic market, and analyzes trafficking and distribution patterns. The report highlights the most current quantitative and qualitative information on drug availability, demand, production and cultivation, transportation, and distribution. The assessment also examines the effects of particular drugs on abusers and society as a whole.

State Drug Threat Assessments provide a detailed threat assessment of drug trends within most states. Each report identifies the primary drug threat in the state and gives a detailed overview of the most current trends by drug type.

Bulletins and briefs are developed in response to new trends or high-priority drug issues. They are quickly relayed to the law enforcement and intelligence communities and warn law enforcement officials of emerging trends. These products are all available on the NDIC web site.

The intelligence analysis staff at NDIC provide strategic and tactical products. The agency has developed software called Realtime Analytic Investigative Database (RAID), which it provides, free of charge, to state and local law enforcement departments. It also provides database training and documentation materials. NDIC staff use RAID when they go into the field to examine documents for major cases.

NDIC also gives training in analysis to personnel at other agencies. It uses distance learning, interactive video training, and other multimedia technologies. Its web site includes access to a number of its threat assessments and bulletins.

National White Collar Crime Center
www.nw3c.org

Through funding from the Bureau of Justice Assistance, the National White Collar Crime Center (NW3C) provides a nationwide support system for agencies involved in the prevention, investigation, and prosecution of economic and high-tech crimes. This nonprofit corporation also supports and partners with other appropriate entities in addressing homeland security initiatives as they relate to economic and high-tech crimes.

NW3C is a member-affiliated organization comprising law enforcement agencies, state regulatory bodies, and state and local prosecution offices. Its growing membership totals more than 1,000 agencies nationwide, and its training programs have delivered up-to-date training in economic and high-tech crime to more than 1,400 agencies.

Through its National Fraud Complaint Management Center (NFCMC) and Internet Crimes Complaint Center (IC3), NW3C provides support services in five main categories: economic and computer crime training, intelligence and analytical services, funding for designated cases, research, and referral and analysis of fraud complaints.

NW3C developed NFCMC to apply technological innovations to the management of economic crime complaints and to improve prevention, investigation, and prosecution efforts resulting from complaints. A significant part of this project was partnering with the FBI to establish IC3. The center represents a unique approach to the growing problem of fraud on the Internet. For law enforcement and regulatory agencies, IC3 offers a central repository for complaints related to Internet fraud, uses the information to quantify fraud patterns, and provides timely statistical data on current fraud trends.

U.S. Department of Homeland Security—Information Analysis and Infrastructure Protection
www.nipc.gov

The Information Analysis and Infrastructure Protection Directorate of the Department of Homeland Security includes publications previously generated and distributed by the National Infrastructure Protection Center of the FBI. Daily reports addressing open-source information are available as are *Cyber Notes.*

U.S. Department of State
www.state.gov

The State Department provides reports on foreign countries, including their history, economy, political situation, population, and leadership ("Background Notes"), which are updated frequently. It also publishes a yearly *Narcotics Control Strategy Report* (last published in March 2004) and *Patterns of Global Terrorism* (last published in April 2004).

U.S. Secret Service
www.secretservice.gov/ntac

The U.S. Secret Service is charged with protecting the president and the vice president, their families, heads of state, and other designated individuals. It plans and implements security designs for designated national special security events. The Secret Service also investigates violations of laws relating to counterfeiting of obligations and securities of the United States; financial crimes that include access device fraud, financial institution fraud, identity theft, and computer fraud; and computer-based attacks on the nation's financial, banking, and telecommunications infrastructure.

It houses the National Threat Assessment Center and has a substantial inventory of assessment products on its web site, which include those listed below:

- *Protective Intelligence and Threat Assessments: A Guide for State and Local Law Enforcement Officials.*
- *Threat Assessment: An Approach to Targeted Violence.*
- *Threat Assessment: Defining an Approach to Evaluating Risk of Targeted Violence.*
- *Threat Assessment in Schools.*
- *Assassination in the United States: An Operational Study of Recent Assassins, Attackers and Near Lethal Approaches.*

Appendix C: Intelligence Training and Resources

Bureau of Justice Assistance
www.ojp.usdoj.gov/BJA

The U.S. Department of Justice (DOJ) Office of Justice Programs' Bureau of Justice Assistance (BJA) provides leadership and services in grant administration and criminal justice policy development to support local, state, and tribal justice strategies to achieve safer communities. BJA's overall goals are to (1) reduce and prevent crime, violence, and drug abuse and (2) improve the functioning of the criminal justice system. To achieve these goals, BJA programs emphasize enhanced coordination and cooperation of federal, state, and local efforts. In the area of intelligence training, BJA provides many intelligence-related resources and training:

- The State and Local Anti-Terrorism Training (SLATT) Program provides specialized counter-terrorism and intelligence training for law enforcement personnel in combating terrorism and extremist criminal activity. For more information, visit www.ojp.usdoj.gov/BJA/tta/index.html.

- The *Criminal Intelligence Systems Operating Policies* (28 C.F.R. Part 23) Training and Technical Assistance program helps law enforcement agencies learn how to comply with the 28 C.F.R. Part 23 guideline. Training courses are half-day, no-cost events held at sites throughout the country.

- The Criminal Intelligence Training for Law Enforcement Chief Executives course assists law enforcement executives in understanding the intelligence function and improving their department's intelligence efforts.

- The National Criminal Intelligence Resource Center (NCIRC) is a new initiative created by BJA to provide support to law enforcement agencies in a secure environment on intelligence policies and procedures, best practices, and training. The NCIRC will be a collaborative effort with other federal agencies involved in intelligence and can be accessed through the RISS network.

- BJA also administers a comprehensive web site that provides access to many other intelligence and information sharing products, including those supported by DOJ's Global Justice Information Sharing Initiative. Visit www.it.ojp.gov to access these resources.

For more information on BJA's training and technical assistance related to information sharing and intelligence, see BJA's Menu of Training Opportunities at www.ojp.usdoj.gov/BJA/tta/index.html.

Counter-Terrorism Training and Resources for Law Enforcement
www.counterterrorismtraining.gov

A product of DOJ and BJA, this web site serves as a single point of access to counter-terrorism training opportunities and related materials available throughout the federal government and from private and nonprofit organizations. Materials cover a wide range of topics, including cyber-terrorism, environmental protection and food and water security, issues relating to first responders and medical response, transportation security, and weapons of mass destruction.

Federal Bureau of Investigation—Virtual Academy
http://fbiva.fbiacademy.edu

The FBI is currently pursuing a project to develop and maintain a web site that will contain intelligence-related information and training information to increase the proficiency levels of street intelligence officers and intelligence analysts.

Federal Law Enforcement Training Center
www.fletc.gov

The Computer and Financial Investigations Division (formerly the Financial Fraud Institute) at the Federal Law Enforcement Training Center (FLETC) has a 72-hour Intelligence Analyst Training Program onsite in Glynco, Georgia. The curriculum includes legal aspects for intelligence personnel, methodology and

analytic skills, research techniques, report writing, collection and documentation of data, identification and document fraud, and information sharing. The course includes hands-on computer and Internet use. An examination is given at the end of the first week of training. The program serves federal, state, and local personnel who are assigned to intelligence or analysis within their agencies or who have a need for intelligence training.

International Association of Chiefs of Police
www.theiacp.org

The International Association of Chiefs of Police (IACP) supports police commanders regarding a range of issues, including intelligence. Its web site contains intelligence policies, information on training workshops, and publications (e.g., the 2002 *Criminal Intelligence Sharing Summit Report, A Police Chief's Primer on Information Sharing,* and *Leading from the Front: Combating and Preparing for Domestic Terrorism).* IACP has been involved in the Criminal Justice Information Sharing project with the Global Intelligence Working Group and the Institute for Intergovernmental Research. IACP provides training on topics of interest to the intelligence field, from organized crime and nontraditional organized crime to undercover operations, informant management, analysis, and principles of report writing.

International Association of Law Enforcement Intelligence Analysts, Inc.
www.ialeia.org

The International Association of Law Enforcement Intelligence Analysts, Inc. (IALEIA), an organization of analysts, intelligence officers, and police managers, was founded in 1980 and has approximately 1,800 members in more than 50 countries. A nonprofit organization dedicated to educating the police community about the benefits of intelligence and analysis, IALEIA trains analysts to meet high standards of professionalism.

In the past decade, it has published a number of documents relating to intelligence and analysis, including:

- *Successful Law Enforcement Using Analytic Methods.*
- *Guidelines for Starting an Analytic Unit.*
- *Intelligence Models and Best Practices.*
- *Intelligence-Led Policing.*
- *Starting an Analytic Unit for Intelligence-Led Policing.*
- *IALEIA Journal 20th Anniversary CD–ROM.*
- *Intelligence 2000: Revising the Basic Elements* (produced jointly with the Law Enforcement Intelligence Unit (LEIU).
- *Turnkey Intelligence: Unlocking Your Agency's Intelligence Capability* (a CD–ROM produced jointly with LEIU and the National White Collar Crime Center).

IALEIA participated in the development of the *Foundations of Intelligence Analysis Training* program (with LEIU, RISS centers, and the National White Collar Crime Center) and offers the course, which is taught by experienced analytic instructors. The IALEIA web site lists available training and reference materials.

Multijurisdictional Counterdrug Task Force Training Program
www.mctft.com

The Multijurisdictional Counterdrug Task Force Training program is a partnership between the Florida National Guard and St. Petersburg (Florida) College. It offers several free courses nationwide, including a basic intelligence analysis course.

New Jersey Division of Criminal Justice
www.njdcj.org

The New Jersey Division of Criminal Justice offers basic, financial, advanced, and strategic analytic training in Trenton, New Jersey. Its courses are free and are open to law enforcement and military personnel.

Office of Community Oriented Policing Services
www.cops.usdoj.gov

The Office of Community Oriented Policing Services (COPS) offers a range of publications and tools to assist with problem-oriented policing and analysis. Its web site has a problem-oriented policing center

(www.popcenter.org) with publications including *Using Analysis for Problem Solving*, "Assessing Responses to Problems: An Introductory Guide for Police Problem Solvers," and other reports and articles, some of which are reprinted from other sources.

COPS also offers documents on intelligence, including:

Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies
(www.cops.usdoj.gov/default.asp?Item=118)
This intelligence guide was prepared in response to requests from law enforcement executives for guidance on intelligence functions in a post-September 11 world. It will help law enforcement agencies develop or enhance their intelligence capacity and enable them to fight terrorism and other crimes while preserving community policing relationships.

"Connecting the Dots for a Proactive Approach"
(www.cops.usdoj.gov/mime/open.pdf?Item=1046)
Community policing is an important part of preparing for and responding to acts of terrorism. This article in *Border and Transportation Security* magazine details the work of three COPS staffers who harness the power of community policing to enhance homeland security.

Protecting Your Community From Terrorism: Strategies for Local Law Enforcement, Volume 4: The Production and Sharing of Intelligence
(www.cops.usdoj.gov/mime/open.pdf?Item=1438)
This document discusses the importance of intelligence-led policing and its correlation with problem-oriented policing principles. The report outlines criteria for an effective intelligence function at all levels of government. Sidebars highlight contributions from key players in the fields of intelligence and policing.

Regional Information Sharing Systems
www.rissinfo.com

RISS centers host a variety of intelligence programs at their sites and in the field. These programs range from those taught by RISS staff members to those taught by experts from federal, state, and local agencies. Many RISS training programs are free or low-cost. Contact the local RISS center for details. (See appendix A for more information about RISS.)

U.S. Department of Homeland Security—Office for Domestic Preparedness
www.ojp.usdoj.gov/odp

The Office for Domestic Preparedness (ODP) is the principal component of the Department of Homeland Security (DHS) responsible for preparing the United States for acts of terrorism. In carrying out its mission, ODP is responsible for providing training, funds for the purchase of equipment, support for the planning and execution of exercises, technical assistance, and other support to assist states and local jurisdictions in preventing, responding to, and recovering from acts of terrorism.

U.S. Drug Enforcement Administration
www.usdoj.gov/dea/programs/training.htm

The U.S. Drug Enforcement Administration manages the Justice Training Center in Quantico, Virginia, which hosts a 4-week Federal Law Enforcement Analytic Training (FLEAT) program for federal, state, and local law enforcement personnel. The FLEAT program is also offered as a 2-week course at HIDTAs nationwide. Contact: 202–305–8500.

Appendix D: Criminal Intelligence Model Policy

Note: A discussion paper is available from the International Association of Chiefs of Police at www.theiacp.org.

Effective Date: June 2003

Subject: Criminal Intelligence

I. Purpose

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

II. Policy

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

It is also the policy of this agency to adopt the standards of the Commission on Accreditation for Law Enforcement Agencies (CALEA) for intelligence gathering, specifically that: If an agency performs an intelligence function, procedures must be established to ensure the legality and integrity of its operations, to include:

- Procedures for ensuring information collected is limited to criminal conduct and relates to activities that prevent a threat to the community.
- Descriptions of the types or quality of information that may be included in the system.
- Methods for purging out-of-date or incorrect information.
- Procedures for the utilization of intelligence personnel and techniques.

The policy contained herein is intended to remain at all times consistent with the current language of 28 C.F.R., Part 23.

III. Definitions

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

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

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

Threshold for Criminal Intelligence. The threshold for collecting information and producing criminal intelligence shall be the "reasonable suspicion" standard in 28 C.F.R., Part 23, Section 23.3 c.

IV. Procedures

A. Mission

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

1. Information gathering in support of the intelligence function is the responsibility of each member of this agency although specific assignments may be made as deemed necessary by the officer-in-charge (OIC) of the intelligence authority.

2. Information that implicates or suggests implication or complicity of any public official in criminal activity or corruption shall be immediately reported to this agency's chief executive officer or another appropriate agency.

B. Organization

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

1. The OIC shall report directly to this agency's chief executive officer or his designate in a manner and on a schedule prescribed by the chief.

2. To accomplish the goals of the intelligence function and conduct routine operations in an efficient and effective manner, the OIC shall ensure compliance with the policies, procedures, mission, and goals of the agency.

C. Professional Standards

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

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

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

3. The intelligence function shall make every effort to ensure that information added to the criminal intelligence base is relevant to a current or ongoing investigation and the product of dependable and trustworthy sources of information. A record shall be kept of the source of all information received and maintained by the intelligence function.

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

D. Compiling Intelligence

1. Intelligence investigations/files may be opened by the intelligence OIC with sufficient information and justification. This includes but is not limited to the following types of information.

   a. subject, victim(s), and complainant as appropriate; summary of suspected criminal activity;

   b. anticipated investigative steps to include proposed use of informants, and photographic or electronic surveillance;

   c. resource requirements, including personnel, equipment, buy/flash monies, travel costs, etc;

   d. anticipated results; and

   e. problems, restraints, or conflicts of interest.

2. Officers shall not retain official intelligence documentation for personal reference or other purposes but shall submit such reports and information directly to the intelligence authority.

3. Information gathering using confidential informants as well as electronic, photographic, and related surveillance devices shall be performed in a legally accepted manner and in accordance with procedures established for their use by this agency.

4. All information designated for use by the intelligence authority shall be submitted on the designated report form and reviewed by the officer's immediate supervisor prior to submission.

E. Analysis

1. The intelligence function shall establish and maintain a process to ensure that information gathered is subjected to review and analysis to derive its meaning and value.

2. Where possible, the above-described process should be accomplished by professional, trained analysts.

3. Analytic material (i.e., intelligence) shall be compiled and provided to authorized recipients as soon as possible where meaningful trends, patterns, methods, characteristics, or intentions of criminal enterprises or individuals emerge.

F. Receipt/Evaluation of Information

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

1. Where possible, information shall be evaluated with respect to reliability of source and validity of content. While evaluation may not be precise, this assessment must be made to the degree possible in order to guide others in using the information. A record shall be kept of the source of all information where known.

2. Reports and other investigative material and information received by this agency shall remain the property of the originating agency, but may be retained by this agency. Such reports and other investigative material and information shall be maintained in confidence, and no access shall be given to another agency except with the consent of the originating agency.

3. Information having relevance to active cases or that requires immediate attention shall be forwarded to responsible investigative or other personnel as soon as possible.

4. Analytic material shall be compiled and provided to authorized sources as soon as possible where meaningful trends, patterns, methods, characteristics, or intentions of criminal enterprises or figures emerge.

G. File Status

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

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

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

H. Classification/Security of Intelligence

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

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

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

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

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

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

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

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

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

I. Auditing and Purging Files

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

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

This project was supported by grant number 2000-DD-VX-0020 awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. The Assistant Attorney General, Office of Justice Programs, coordinates the activities of the following program offices and bureaus: the Bureau of Justice Assistance, the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the U.S. Department of Justice or the International Association of Chiefs of Police.

Endnotes

[1] Dintino and Martens, p. 58.

[2] Federal Bureau of Investigation, p. 319.

[3] Godfrey and Harris, p. 2.

[4] Ibid., p. 28.

[5] Peterson, 2002, "Basics of Intelligence Revisited," p. 3.

[6] McDowell, pp. 12–13.

[7] National Criminal Intelligence Service UK, p. 11.

[8] Marynik, p. 22.

[9] National Advisory Committee on Criminal Justice Standards and Goals, p. 250.

[10] Ibid.

[11] California Peace Officers' Association, 1988, p. 4.

[12] King, 2002, p. 79.

[13] Godfrey and Harris, p. 23.

[14] Harris, p. 27.

[15] Robert C. Fahlman and Marilyn B. Peterson, 1997, "From Conclusions to Recommendations: The Next Step," *IALEIA Journal* 10(2):26–28.

[16] Dintino and Martens, p. 115.

[17] Godfrey and Harris, p. 29.

[18] Ibid., p. 21.

[19] Anderson, p. 5.

[20] Ibid., p. 6.

[21] Ibid., p. 8.

[22] Iowa Department of Public Safety, p. 13.

[23] Ibid., pp. 20–27.

[24] National Criminal Intelligence Service UK, p. 8.

[25] Ibid., p. 9.

[26] Peterson, 2002, "Toward a Model for Intelligence-Led Policing in the United States," p. 5.

[27] Goldstein, 1990.

[28] Goldstein, 2003, p. 14.

[29] Clarke and Eck, p. 2.

[30] Peterson, 2002, "Local and State Anti-Terrorism Analysis," p. 79.

[31] Goldstein, 1990, p. 27.

[32] Ibid., pp. 28–29.

[33] Scheider and Chapman, p. 3.

[34] Ibid., p. 2.

[35] Wright, 2001, p. 69.

[36] Ibid., p. 70.

[37] Wright, 1998, p. 1.

[38] *National Criminal Intelligence Sharing Plan*, retrieved from http://it.ojp.gov/topic.jsp?topic_id=93, August 15, 2003.

[39] California Peace Officers' Association, 1998, p. 8.

[40] Global Intelligence Working Group, 2003, pp. 35–40.

[41] New Jersey Department of Law and Public Safety, Statewide Intelligence Training Strategy Working Group, p. 12.

[42] Ibid., p. 22.

[43] National Advisory Committee on Criminal Justice Standards and Goals, p. 250.

[44] International Association of Law Enforcement Intelligence Analysts, p. 4.

[45] Ibid., p. 66.

[46] Ibid., p. 6.

[47] Godfrey and Harris, p. 92.

[48] Ibid., p. 98.

[49] Ibid., p. 94.

[50] Global Intelligence Working Group, 2003, p. 50.

[51] National White Collar Crime Center.

[52] Two exceptions are Pennsylvania and New Jersey. Pennsylvania has a law on criminal intelligence, and New Jersey has *Attorney General Intelligence Guidelines* (available at www.njdcj.org/agguide/intelligence.pdf).

[53] Bureau of Justice Assistance, p. 4.

[54] Ibid., pp. 12–16.

[55] Ibid., p. 22.

[56] National Law Enforcement Policy Center, 2003, p. v.

[57] U.S. Department of Justice, p. 2.

[58] Dintino and Martens, p. 123.

[59] Godfrey and Harris, p. 21.

[60] Federal Bureau of Investigation, p. 330.

[61] Porter, pp. 23–27.

[62] Office of Community Oriented Policing Services, pp. 11–14

[63] Council on Counter-Narcotics, p. 37.

Bibliography

The 9/11 Commission. 2004. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States.* 2004. New York, NY: Norton & Co.

Anderson, Richard. 1997. "Intelligence-Led Policing: A British Perspective." In *Intelligence Led Policing: International Perspectives on Policing in the 21st Century.* Lawrenceville, NJ: International Association of Law Enforcement Intelligence Analysts.

Bouza, Anthony V. 1976. *Police Intelligence—The Operations of an Investigative Unit.* New York, NY: AMS Press.

Bureau of Justice Assistance. 1998. *The Statewide Intelligence Systems Program.* Washington, DC: U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance.

Bynum, Timothy S. 2001. *Using Analysis for Problem Solving: A Guidebook for Law Enforcement.* Washington, DC: U.S. Department of Justice, Office of Justice Programs, Office of Community Oriented Policing Services.

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

———. 1998. *Criminal Intelligence Program for the Smaller Agency.* Sacramento, CA: California Peace Officers' Association.

Clarke, Ronald V., and John Eck. 2003. *Become a Problem-Solving Crime Analyst in 55 Small Steps.* London, England: Jill Dando Institute of Crime Science.

Council on Counter-Narcotics. 2000. *General Counterdrug Intelligence Plan.* Retrieved July 23, 2005 from www.whitehousedrugpolicy.gov/publications/gcip/gcip.pdf.

Dintino, Justin J., and Frederick T. Martens. 1983. *Police Intelligence Systems in Crime Control.* Springfield, IL: Charles C Thomas.

Fahlman, Robert C., and Marilyn B. Peterson. 1997. "Developing Recommendations: The Next Step in Analysis." *IALEIA Journal* 10(2):25-35.

Federal Bureau of Investigation. 2002. *Crime in the United States.* Washington, DC: Federal Bureau of Investigation.

Global Intelligence Working Group. 2004. "10 Simple Steps To Help Your Agency Become a Part of the *National Criminal Intelligence Sharing Plan.*" Revised brochure. Washington, DC: U.S. Department of Justice, Office of Justice Programs.

———. 2003. *National Criminal Intelligence Sharing Plan.* Washington, DC: U.S. Department of Justice, Office of Justice Programs.

Global Justice Information Sharing Initiative. 2003. *Applying Security Practices to Justice Information Sharing.* CD–ROM. Washington, DC: U.S. Department of Justice, Office of Justice Programs.

Godfrey, E. Drexel, and Don R. Harris. 1971. *Basic Elements of Intelligence.* Washington, DC: U.S. Department of Justice, Office of Criminal Justice Assistance, Law Enforcement Assistance Administration.

Goldstein, Herman. 2003. "On Further Developing Problem-Oriented Policing: The Most Critical Need, the Major Impediments, and a Proposal." *Crime Prevention Studies* 15:13–57.

———. 1990. *Problem-Oriented Policing.* Philadelphia, PA: Temple University Press.

Harris, Don R. 1976. *Basic Elements of Intelligence–Revised.* Washington, DC: U.S. Department of Justice, Office of Criminal Justice Assistance, Law Enforcement Assistance Administration.

International Association of Law Enforcement Intelligence Analysts. 2001. *Starting an Analytic Unit for Intelligence-Led Policing,* edited by M. Peterson. Lawrenceville, NJ: International Association of Law Enforcement Intelligence Analysts.

Iowa Department of Public Safety. 2004. "Iowa Fusion Center Concept." PowerPoint presentation. Retrieved July 23, 2005 from www.iowahomelandsecurity.org.

King, John W. "Collection." 2001. In *Intelligence 2000: Revising the Basic Elements,* edited by M.B. Peterson, B. Morehouse, and R. Wright. Lawrenceville, NJ: International Association of Law Enforcement Intelligence Analysts and Law Enforcement Intelligence Unit.

———. *Criminal Intelligence File Guidelines. 2002.* Sacramento, CA: Law Enforcement Intelligence Unit.

Martens, Frederick T. 2001. "Use, Misuse and Abuse of Intelligence." In *Intelligence 2000: Revising the Basic Elements.* Lawrenceville, NJ: International Association of Law Enforcement Intelligence Analysts and Law Enforcement Intelligence Unit.

Marynik, Jerry. 1998. *Threat Assessment Guide: Evaluating and Analyzing Criminal Extremist Groups.* Sacramento, CA: California Department of Justice.

McDowell, Don. 1998. *Strategic Intelligence: A Handbook for Practitioners, Managers, and Users.* Cooma, Australia: Istana Enterprises Pty. Ltd.

National Advisory Committee on Criminal Justice Standards and Goals. 1973. *Police.* Washington, DC: U.S. Department of Justice, Office of Criminal Justice Assistance, Law Enforcement Assistance Administration.

National Criminal Intelligence Service UK. 2000. *The National Intelligence Model.* London, England: National Criminal Intelligence Service.

National Criminal Justice Association. 2002. *Justice Information Privacy Guidelines.* Washington, D.C.: National Criminal Justice Association.

National Law Enforcement Policy Center. 2003. *Criminal Intelligence Model Policy.* Alexandria, VA: International Association of Chiefs of Police.

———. 2002. *Criminal Intelligence Sharing Summit Report.* Alexandria, VA: International Association of Chiefs of Police.

———. 2000. *Toward Improved Criminal Justice Information Sharing: An Information Integration Planning Model.* Alexandria, VA.: International Association of Chiefs of Police.

National White Collar Crime Center. *Securing Law Enforcement Computer Systems for Law Enforcement Executives and Managers.* CD–ROM. Richmond, VA: International Association of Chiefs of Police and National White Collar Crime Center.

New Jersey Department of Law and Public Safety, Statewide Intelligence Training Strategy Working Group. 2004. *Statewide Intelligence Training Strategy.* Trenton, NJ: New Jersey Department of Law and Public Safety.

Office of Community Oriented Policing Services. 2003. *Promising Strategies From the Field: Community Policing in Smaller Jurisdictions.* Washington, DC: U.S. Department of Justice, Office of Justice Programs, Office of Community Oriented Policing Services.

Peterson, Marilyn B. 2002. "The Basics of Intelligence Revisited." In *Turnkey Intelligence: Unlocking Your Agency's Intelligence Capability.* Richmond, VA: International Association of Law Enforcement Intelligence Analysts, Law Enforcement Intelligence Unit, and National White Collar Crime Center.

———. 2002. "Local and State Anti-Terrorism Analysis." *Illinois Law Enforcement Executive Institute Forum* 2(1): 78-84.

———. 2002. "Strategic Targeting & Prioritization: A Pro-Active Approach to Targeting Criminal Activity." *Intersec: The Journal of International Security* 12(May):161–163.

———. 2002. “Toward a Model for Intelligence-Led Policing in the United States.” In *Turnkey Intelligence: Unlocking Your Agency’s Intelligence Capability.* CD–ROM. Lawrenceville, NJ: International Association of Law Enforcement Intelligence Analysts, Law Enforcement Intelligence Unit, and National White Collar Crime Center.

Peterson, Marilyn, Bob Morehouse, and Richard Wright, eds. 2001. *Intelligence 2000: Revising the Basic Elements.* Lawrenceville, NJ: International Association of Law Enforcement Intelligence Analysts and Law Enforcement Intelligence Unit.

Porter, Russell M. 1999. “Iowa’s LEIN Program Offers Law Enforcement Excellence Through Cooperation.” In *Intelligence Models and Best Practices,* edited by A. Hopkinson. Lawrenceville, NJ: International Association of Law Enforcement Intelligence Analysts.

Rogovin, Charles H. 2003. “The Analyst’s Role in Creating Strategy.” Paper presented at the International Conference on Organized Crime in Belfast, Northern Ireland, June 11–13, 2003.

Scheider, Matthew C., and Robert Chapman. 2003. “Community Policing and Terrorism.” In *Homeland Security Journal, 2003*. Retrieved July 28, 2005 from www.homelandsecurity.org/journal/articles/Scheider-Chapman.html.

U.S. Department of Justice. 2004. “Law Enforcement Information Sharing Strategy.” Draft. Washington, DC: U.S. Department of Justice.

Wright, Richard. 2001. “Management of the Intelligence Unit.” In *Intelligence 2000: Revising the Basic Elements,* edited by Marilyn B. Peterson, Richard Wright, and Bob Morehouse. Lawrenceville, NJ: International Association of Law Enforcement Intelligence Analysts and Law Enforcement Intelligence Unit.

———. 1998. “Ten Steps to Establishing a Criminal Intelligence Unit.” In *Issues of Interest to Law Enforcement, Criminal Intelligence: A Vital Police Function*, edited by Marilyn B. Peterson. Sacramento, CA: Law Enforcement Intelligence Unit.

Bureau of Justice Assistance Information

BJA's mission is to provide leadership and services in grant administration and criminal justice policy to support local, state, and tribal justice strategies to achieve safer communities. For more indepth information about BJA, its programs, and its funding opportunities, contact:

Bureau of Justice Assistance
810 Seventh Street NW.
Washington, DC 20531
202–616–6500
Fax: 202–305–1367
www.ojp.usdoj.gov/BJA
E-mail: AskBJA@usdoj.gov

The BJA Clearinghouse, a component of the National Criminal Justice Reference Service, shares BJA program information with federal, state, local, and tribal agencies and community groups across the country. Information specialists provide reference and referral services, publication distribution, participation and support for conferences, and other networking and outreach activities. The clearinghouse can be contacted at:

Bureau of Justice Assistance Clearinghouse
P.O. Box 6000
Rockville, MD 20849–6000
1–800–851–3420
Fax: 301–519–5212
www.ncjrs.gov
Send questions or comments to *http://www.ncjrs.gov/App/ContactUs.aspx*.

Clearinghouse staff are available Monday through Friday, 10 a.m. to 6 p.m. eastern time. Ask to be placed on the BJA mailing list.

To subscribe to the electronic newsletter *JUSTINFO* and become a registered NCJRS user, visit *http://ncjrs.gov/subreg.html*.

BJA