



United States  
Department of Justice

# MINIMUM CRIMINAL INTELLIGENCE TRAINING STANDARDS

for Law Enforcement and  
Other Criminal Justice Agencies in the United States

Findings and Recommendations

October 2007  
Version 2

## **About Global**

The U.S. Department of Justice's Global Justice Information Sharing Initiative (Global) serves as a Federal Advisory Committee to the U.S. Attorney General on critical justice information sharing initiatives. Global promotes standards-based electronic information exchange to provide justice and public safety communities with timely, accurate, complete, and accessible information in a secure and trusted environment. Global is administered by the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance.



This project was supported by Grant No. 2007-MU-BX-K002 awarded by the Bureau of Justice Assistance. 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. 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.

# MINIMUM CRIMINAL INTELLIGENCE TRAINING STANDARDS

For Law Enforcement and Other  
Criminal Justice Agencies in the United States

Findings and Recommendations

October 2007  
Version 2

## TABLE OF CONTENTS

Introduction .....	1
Philosophy .....	1
Understanding Minimum Standards.....	1
Curricula.....	2
Additional Criminal Intelligence Training .....	2
Intelligence Analyst .....	3
Summary .....	3
Objective I .....	4
Objective II.....	4
Objective III.....	5
Objective IV.....	5
Objective V.....	5
Objective VI.....	6
Objective VII .....	6
Objective VIII.....	6
Intelligence Manager/Commander.....	7
Summary .....	7
Objective I .....	8
Objective II.....	8
Objective III.....	9
Objective IV.....	10
Objective V.....	10
Objective VI.....	11
Law Enforcement Executive .....	13
Summary .....	13
Objective I .....	14
Objective II.....	14
Objective III.....	14
Objective IV.....	15
Objective V.....	15
General Law Enforcement Officer—Basic Criminal Intelligence.....	17
Summary .....	17
Objective I .....	18
Objective II.....	18
Objective III.....	19
Objective IV.....	19

General Law Enforcement Officer—Criminal Intelligence Refresher .....	21
Summary .....	21
Objective I .....	22
Objective II .....	22
Objective III .....	23
Objective IV .....	23
Criminal Intelligence Officer .....	25
Summary .....	25
Objective I .....	26
Objective II .....	27
Objective III .....	27
Objective IV .....	28
Objective V .....	28
Objective VI .....	29
Objective VII .....	29
Train-the-Trainer .....	31
Summary .....	31
Objective I .....	32
Objective II .....	32
Objective III .....	33
Objective IV .....	33
Objective V .....	33
Objective VI .....	34
Objective VII .....	34
Objective VIII .....	34
Appendix .....	35

---

## INTRODUCTION

---

The intent of this document is to provide perspective and guidance for the development and delivery of law enforcement intelligence training. It is recognized that any type of “standard” can be debated based on an individual’s personal philosophy, professional priorities, and life experiences. In order to minimize bias or atypical context, the development process for these standards used a consensual approach reflecting the cumulative judgment of law enforcement intelligence practitioners, managers, executives, trainers, and scholars from all levels of government.

The standards reflect the collective judgment of these subject-matter experts (SMEs) with respect to the minimum training needed in each noted classification to provide the basic knowledge, skills, and abilities for personnel in each classification in order for them to perform their intelligence duties. In particular for the intelligence analyst, those duties would be at the entry level.

This document should be viewed as a “living document” because supplements may be developed in the future. Future supplements may address additional training classifications or other specialized training needs based on threats that, although not criminal, have implications for homeland security. Individuals and organizations are invited to submit recommendations for future versions of this document via the National Criminal Intelligence Resource Center ([www.ncirc.gov](http://www.ncirc.gov)) e-mail address: [information@ncirc.gov](mailto:information@ncirc.gov).

---

## PHILOSOPHY

---

These minimum standards were created within the context of the following statement of philosophy as applied to all training categories:

*This training is designed to develop a culture of information analysis and information sharing within the law enforcement communities for the purpose of safeguarding America’s communities while protecting citizens’ privacy and civil rights.*

---

## UNDERSTANDING MINIMUM STANDARDS

---

The SMEs who developed these standards expressed the need to reinforce the fact that these are minimum training standards. Personnel who attend training that meets these standards will possess core competencies to perform their duties lawfully and effectively. Of course, effectiveness and efficiency will increase with both experience and additional training.

Program developers are urged to expand the modules’ content and times as practicable. This is particularly true as new laws, issues, trends, and best practices emerge. Standards are dynamic, reflecting the best knowledge at the time they are written; monitoring changes within the training environment is a critical responsibility of training program developers.

Permeating each component of the training should be the consideration of issues related to fusion centers, the Information Sharing Environment (ISE), privacy issues, and community policing, as applicable to each component of the training.

The minimum standards outlined in this document are recommendations for core minimum criminal intelligence training standards for each training classification:

- Intelligence Analyst
- Intelligence Manager/Commander

- Law Enforcement Executive
- General Law Enforcement Officer—Basic Criminal Intelligence
- General Law Enforcement Officer—Criminal Intelligence Refresher
- Criminal Intelligence Officer
- Train-the-Trainer

The recommendations include objectives, standards, and suggested curriculum/sources of information, as well as time allocations. Standards are defined as specific courses or topics of instruction required to meet the training objective.

## CURRICULA

---

Program developers are reminded that the minimum standards are not curricula. The standards represent topics for which curricula are developed. A suggested curriculum and sources of information are included for each standard. The SMEs who developed these standards made one overarching recommendation regarding curricula.

- Curricula content should include the latest iteration of national standards for law enforcement intelligence (e.g., the *National Criminal Intelligence Sharing Plan* (NCISP) and the *Information Sharing Environment Implementation Plan*) as well as the most current developments in the field (e.g., new regulations, emerging privacy guidelines and/or state-specific requirements, new technologies, and intelligence resources).

Curricula structure should be based on accepted principles of adult learning. These include methods to evaluate learning, such as pre- and posttests; problem-solving exercises; and/or demonstration of learning objective mastery.

## ADDITIONAL CRIMINAL INTELLIGENCE TRAINING

---

The training categories contained in this document are drawn from those articulated in the NCISP and are dependent largely on a person's specific assignment in a law enforcement organization. It is recognized there are important and relevant intelligence training programs that are not covered by the standards; for example, programs for developing an intelligence capacity in a law enforcement agency, new programs focused specifically on intelligence-led policing, or a program on public/private partnerships for the intelligence process and the ISE. Similarly, new programs may target specific issues, such as gang intelligence or drug intelligence. These programs are important and have value despite the lack of specifically defined minimum standards. Collaborative efforts with other criminal justice agencies, such as corrections and parole and probation, may also result in additional topics in the future.

Program developers are urged to explore the diverse applications of law enforcement intelligence where training voids exist. In those programs, developers are also urged to adopt the same philosophy and curricular issues described above.

## INTELLIGENCE ANALYST

Time Allotment: 40 hours minimum

Time Allotment per Objective:

<b>3 hours</b>	<b>Objective I:</b>	Intelligence analysts will understand the criminal intelligence process, intelligence-led policing, the information sharing framework, and their roles in enhancing public safety.
<b>2 hours</b>	<b>Objective II:</b>	Analysts will gain an understanding of the proper handling and collation of criminal intelligence information, including file management and information evaluation.
<b>4 hours</b>	<b>Objective III:</b>	Analysts will experience the development of intelligence through the processes of critical thinking, logic, inference development, and recommendation development.
<b>2–3 hours</b>	<b>Objective IV:</b>	Analysts will understand the methodical process of developing and implementing collection and analytic plans, to include the reevaluation of that process/product.
<b>2–3 hours</b>	<b>Objective V:</b>	Analysts will be familiar with the legal, privacy, and ethical issues relating to intelligence.
<b>3 hours</b>	<b>Objective VI:</b>	Analysts will be provided with information on sources, including the Internet, information sharing systems, networks, centers, commercial and public databases, and other sources of information and their limitations.
<b>16 hours</b>	<b>Objective VII:</b>	Analysts will be able to demonstrate a practical knowledge of the methods, tools, and techniques employed in analysis.
<b>4–8 hours</b>	<b>Objective VIII:</b>	Analysts will be familiar with the skills underlying analytic methods, including report writing, statistics, and graphic techniques.

\*It is recommended that the most current developments in the field (e.g., fusion centers, *Information Sharing Environment (ISE) Implementation Plan (IP)*, and updated terminology) be referenced in the curriculum for each training objective.

### SUMMARY

The role of the intelligence analyst is more critical than ever as we move to a systemic model involving the ISE. Analysts have more diverse information and are required to produce more explicit tactical and strategic intelligence products. There are demands for threat assessments and the need to prepare intelligence reports that are in a form easily consumed, not only by intelligence professionals but also by line-level law enforcement officers. The Minimum Criminal Intelligence Training Standards for the Intelligence Analyst must incorporate these elements if the conceptual model for intelligence fusion and the Information Sharing Environment (see Appendix) is going to reach fruition. Thus, these standards include new and emerging responsibilities for the intelligence analyst that are necessary throughout the law enforcement intelligence community.

**Objective I:** Intelligence analysts will understand the criminal intelligence process, intelligence-led policing, the information sharing framework, and their roles in enhancing public safety.

3 hours	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Introduction to intelligence	
	2. Intelligence process/cycle	<ul style="list-style-type: none"> <li>• Collection, analysis, dissemination/production, collation, evaluation, assessment</li> <li>• Origin/history of intelligence</li> <li>• Roles and responsibilities of the analyst</li> <li>• Intelligence-led policing</li> </ul>
	3. Networking	<ul style="list-style-type: none"> <li>• Liaise with peers, other agencies, organizations, and professional memberships for dissemination of information</li> </ul>
	4. Importance of the <i>National Criminal Intelligence Sharing Plan</i> (NCISP)	<ul style="list-style-type: none"> <li>• Information sharing/information sharing initiatives (LEISP, Global, N-DEx) (Curriculum developers should include current initiatives and those of local and/or regional importance.)</li> <li>• Threats facing community, state, nation</li> <li>• Terrorism/topical materials</li> <li>• Intelligence-led policing</li> <li>• Community policing</li> </ul>
	5. Professional standards/certification program for analysts	<ul style="list-style-type: none"> <li>• International Association of Law Enforcement Intelligence Analysts</li> <li>• <i>Law Enforcement Analytic Standards</i></li> <li>• International Association of Crime Analysts</li> </ul>
	6. Information sharing framework	<ul style="list-style-type: none"> <li>• Fusion centers, ISE IP, and local/regional initiatives</li> </ul>

**Objective II:** Analysts will gain an understanding of the proper handling and collation of criminal intelligence information, including file management and information evaluation.

2 hours	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Security	<ul style="list-style-type: none"> <li>• LEIU <i>Criminal Intelligence File Guidelines</i></li> <li>• <a href="http://www.iooss.gov/">www.iooss.gov/</a></li> </ul>
	2. Information management	<ul style="list-style-type: none"> <li>• Electronic</li> <li>• Archives (storage)</li> <li>• Files (hard copy)</li> </ul>
	3. Evaluation	<ul style="list-style-type: none"> <li>• Reliability/source validity</li> </ul>
	4. Markings and using confidential information	<ul style="list-style-type: none"> <li>• Classified</li> <li>• Sensitive But Unclassified (SBU)</li> <li>• Proposed Controlled Unclassified Information (CUI) framework</li> <li>• State-authorized markings</li> </ul>

**Objective III:** Analysts will experience the development of intelligence through the processes of critical thinking, logic, inference development, and recommendation development.

4 hours	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Critical thinking	
	2. Logical/fallacies of logic	
	3. Inference development	<ul style="list-style-type: none"> <li>• Carter, David L. (1994). <i>Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies</i>. Washington, DC. U.S. Department of Justice.</li> </ul>
	4. Crime indicators	
	5. Crime patterns/analysis	

**Objective IV:** Analysts will understand the methodical process of developing and implementing collection and analytic plans, to include the reevaluation of that process/product.

2-3 hours	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Needs of the consumer (strategic, tactical)	<ul style="list-style-type: none"> <li>• Does the intelligence product meet the needs of its intended purpose?</li> </ul>
	2. Intelligence requirements/collection	<ul style="list-style-type: none"> <li>• Intelligence gaps</li> <li>• Intelligence requirements</li> <li>• Global's state, local, and tribal intelligence requirements</li> </ul>
	3. Effective planning of intelligence products	<ul style="list-style-type: none"> <li>• Development of collection and investigative plans</li> </ul>
	4. Infusing consumer feedback into the intelligence cycle	

**Objective V:** Analysts will be familiar with the legal, privacy, and ethical issues relating to intelligence.

2-3 hours	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Law and legal aspects	<ul style="list-style-type: none"> <li>• Adhering to policies/procedures</li> <li>• 28 CFR Part 23</li> <li>• Possible resources include U.S. Attorneys' Offices, District Attorneys' Offices, and local prosecutors</li> </ul>
	2. Privacy, civil liberties, and civil rights	<ul style="list-style-type: none"> <li>• Include privacy issues/examples</li> </ul>
	3. Ethics	<ul style="list-style-type: none"> <li>• Provide scenario to illustrate importance</li> </ul>
	4. Civil liability	<ul style="list-style-type: none"> <li>• Overview of liability issues in the intelligence process</li> </ul>

**Objective VI:** Analysts will be provided with information on sources, including the Internet, information sharing systems, networks, centers, commercial and public databases, and other sources of information and their limitations.

3 hours	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Sources of information/available resources	<ul style="list-style-type: none"> <li>• Law enforcement and intelligence information systems, such as RISS, HSIN, and LEO</li> <li>• Corrections and other criminal justice information systems</li> <li>• Open source information</li> <li>• Demonstration of selected systems</li> </ul>

**Objective VII:** Analysts will be able to demonstrate a practical knowledge of the methods, tools, and techniques employed in analysis.

16 hours	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Analytical techniques	<ul style="list-style-type: none"> <li>• Threat assessments</li> <li>• Crime pattern analysis</li> <li>• Association analysis</li> <li>• Telephone record analysis</li> <li>• Flowchart analysis (event/commodity)</li> <li>• Financial analysis</li> <li>• Strategic analysis</li> </ul>
2. Analytical tools	<ul style="list-style-type: none"> <li>• Spreadsheets</li> <li>• Flowcharting applications</li> <li>• Analytic software</li> <li>• Presentation software, etc.</li> </ul>	

**Objective VIII:** Analysts will be familiar with the skills underlying analytic methods, including report writing, statistics, and graphic techniques.

4-8 hours	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Report writing	<ul style="list-style-type: none"> <li>• Principles of good report writing</li> <li>• Differences between intelligence/ investigative reports, briefs, etc.</li> </ul>
2. Presentation of information	<ul style="list-style-type: none"> <li>• Oral and written briefings</li> </ul>	

## INTELLIGENCE MANAGER/COMMANDER

Time Allotment: 16 hours minimum

Time Allotment per Objective:

<b>3 hours</b>	<b>Objective I:</b>	Managers will understand the criminal intelligence process, intelligence-led policing, and their roles in enhancing public safety.
<b>2 hours</b>	<b>Objective II:</b>	Managing the Intelligence Unit. Managers will understand the personnel and policy considerations when establishing or assuming command of the intelligence function within an agency.
<b>2 hours</b>	<b>Objective III:</b>	Managers will understand the principles and practices of handling sensitive information, informant policies, and corruption prevention and recognition.
<b>3 hours</b>	<b>Objective IV:</b>	Managers will understand the legal and privacy issues surrounding the criminal intelligence environment.
<b>4 hours</b>	<b>Objective V:</b>	Managers will understand the processes necessary to produce tactical and strategic intelligence products and will understand the development process and implementation of collection plans.
<b>2 hours</b>	<b>Objective VI:</b>	Managers will be provided with information on criminal information sharing systems, networks, and resources available to their agencies.

\*It is recommended that the most current developments in the field (e.g., fusion centers, *Information Sharing Environment (ISE) Implementation Plan (IP)*, and updated terminology) be referenced in the curriculum for each training objective.

### SUMMARY

Law enforcement managers/commanders are often assigned to a new position without having any experience or substantive knowledge of the new area of responsibility. There is an old administrative adage from the auto industry that an effective manager does not have to know how to build a car but must know how others build a car. Although there is some truth to this, lessons learned have shown us that when managers have substantive knowledge of the processes under their supervision, they are even more effective managers. Law enforcement intelligence is a politically and constitutionally sensitive area that requires a manager to understand the responsibilities, hazards, and challenges of the intelligence process. The Minimum Criminal Intelligence Training Standards for Intelligence Managers/Commanders are not designed to teach management; rather, they are designed to give managers critical knowledge of the law enforcement intelligence process to not only maximize their leadership capabilities but also prepare them for the unique challenges faced by personnel under the manager's command.

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

3 hours	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Intelligence purpose/mission	<ul style="list-style-type: none"> <li>• Where does intelligence fit in your agency?</li> <li>• Roles/responsibilities of intelligence function</li> <li>• Provide examples of intelligence function missions</li> <li>• Write a mission for your intelligence function</li> </ul>
	2. Importance of the NCISP	<ul style="list-style-type: none"> <li>• Information sharing/information sharing initiatives (LEISP, Global, N-DEx) (Curriculum developers should include current initiatives and those of local and/or regional importance.)</li> <li>• Threats facing community, state, nation</li> <li>• Terrorism/topical materials</li> <li>• Intelligence-led policing</li> <li>• Community policing</li> </ul>
	3. Definition of “intelligence”	<ul style="list-style-type: none"> <li>• Examples of what it is/what it is not</li> <li>• Do not rely on one definition</li> </ul>
	4. General intelligence process/cycle	<ul style="list-style-type: none"> <li>• Include impediments to the intelligence process/cycle</li> </ul>
	5. Why intelligence is important to managers, analysts, executives	<ul style="list-style-type: none"> <li>• Focus on why intelligence is important for the agency and community you serve</li> </ul>
	6. Intelligence-led policing	<ul style="list-style-type: none"> <li>• Brief overview/definitions of “intelligence-led policing”</li> <li>• Community-oriented policing</li> </ul>
	7. Information sharing network	<ul style="list-style-type: none"> <li>• Fusion centers, ISE IP, and local/regional initiatives</li> </ul>

**Objective II:** Managing the Intelligence Unit. Managers will understand the personnel and policy considerations when establishing or assuming command of the intelligence function within an agency.

2 hours	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Personnel selection	<ul style="list-style-type: none"> <li>• Background process consistent with NCISP</li> </ul>
	2. Personnel training	<ul style="list-style-type: none"> <li>• Informative component; include what executives, analysts, and officers should be trained on and where training is available</li> </ul>
	3. Personnel evaluation	<ul style="list-style-type: none"> <li>• Evaluate personnel unique to the intelligence function to the extent possible</li> </ul>

**Objective II:** (continued)

2 hours (continued)	Standards	Topics to Be Considered for Curriculum/Sources of Information
	4. Evaluating intelligence unit performance	<ul style="list-style-type: none"> <li>• Does the mission/scope of the unit match the products produced?</li> <li>• Is there effective communication within the law enforcement organization and with consumers?</li> <li>• CALEA and other applicable national and state standards</li> <li>• Provide handout/checklist; include:                             <ul style="list-style-type: none"> <li>• Production of bulletins</li> <li>• Analysis of threats</li> <li>• Information regarding performance metrics</li> <li>• Training of unique measures related to criteria unique to the intelligence process</li> <li>• Evaluation tied to the mission</li> </ul> </li> </ul>
5. Operating policies and procedures—mechanics of an intelligence function	<ul style="list-style-type: none"> <li>• Physical security</li> <li>• File management</li> <li>• Informants</li> <li>• Ethics</li> <li>• Handouts/CDs (e.g., glossary)</li> </ul>	

**Objective III:** Managers will understand the principles and practices of handling sensitive information, informant policies, and corruption prevention and recognition.

2 hours	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Handling and storing of information (security, e-mail)	<ul style="list-style-type: none"> <li>• Internet, networks/systems, firewalls</li> </ul>
	2. Classifications	<ul style="list-style-type: none"> <li>• Secret, Top Secret, national security issues (pamphlets from FBI, etc.)</li> </ul>
	3. Operational security processes	<ul style="list-style-type: none"> <li>• Protecting methods and sources</li> <li>• Policies/rules (i.e., dissemination)</li> <li>• Disclosure of sensitive information to media, other law enforcement entities, citizens, public safety agencies, etc.</li> </ul>
	4. Markings and using confidential information	<ul style="list-style-type: none"> <li>• Classified</li> <li>• Sensitive But Unclassified (SBU)</li> <li>• Proposed CUI framework</li> <li>• State-authorized markings</li> </ul>

**Objective IV:** Managers will understand the legal and privacy issues surrounding the criminal intelligence environment.

3 hours	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Legal and historical perspectives	<ul style="list-style-type: none"> <li>• Historical abuses of civil rights due to antiquated law enforcement practices</li> <li>• Provide examples or scenarios that illustrate the importance of legal/privacy issues</li> <li>• Include issues/examples regarding privacy</li> <li>• Possible resources include U.S. Attorneys' Offices, District Attorneys' Offices, and local prosecutors</li> </ul>
	2. Current regulations	<ul style="list-style-type: none"> <li>• Regulations/resources on CD (28 CFR Part 23)</li> </ul>
	3. Application	<ul style="list-style-type: none"> <li>• Question-and-answer session</li> <li>• How to put this information into practice</li> </ul>
	4. Ensuring accountability	<ul style="list-style-type: none"> <li>• Provide a checklist to gauge compliance (LEIU Checklist copies)</li> </ul>
	5. Privacy	<ul style="list-style-type: none"> <li>• Privacy policy development</li> <li>• <i>Global Privacy and Civil Liberties Policy Development Guide and Implementation Templates</i></li> </ul>
	6. Ethics	<ul style="list-style-type: none"> <li>• Review IACP code of conduct and agency-specific or recognized code of ethics</li> </ul>

**Objective V:** Managers will understand the processes necessary to produce tactical and strategic intelligence products and will understand the development process and implementation of collection plans.

4 hours	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Defining the customers	<ul style="list-style-type: none"> <li>• Understand the needs of the customer and what is important to the customer</li> </ul>
	2. Methods of collection	<ul style="list-style-type: none"> <li>• Identifying gaps</li> </ul>
	3. Competing hypotheses	<ul style="list-style-type: none"> <li>• Reliability/validity—ensure that analysis is reliable; do not follow a blind alley</li> </ul>
	4. Types of intelligence products and analytic techniques	<ul style="list-style-type: none"> <li>• Discuss the various intelligence products available to the agency</li> <li>• Planning for intelligence products</li> <li>• Threat assessments</li> <li>• Strategic, tactical, operational, data visualization</li> <li>• Discuss the value of products</li> </ul>
	5. Principles of good report writing	<ul style="list-style-type: none"> <li>• Provide differences between intelligence/investigative projects/reports, briefs, etc.</li> </ul>
6. Feedback	<ul style="list-style-type: none"> <li>• Does the intelligence product meet the needs of its intended purpose?</li> </ul>	

**Objective VI:** Managers will be provided with information on criminal information sharing systems, networks, and resources available to their agencies.

2 hours	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Sources of information/available resources	<ul style="list-style-type: none"> <li>• Provide overview, resource CD</li> <li>• Law enforcement and intelligence information systems</li> <li>• Open source information (inclusive of criminal history, RISS)</li> <li>• Demonstration of selected systems</li> </ul>
2. Networking/relationship building	<ul style="list-style-type: none"> <li>• Discuss how intelligence is not only technical, it is a human effort</li> <li>• Provide information on associations/networking opportunities</li> </ul>	



## LAW ENFORCEMENT EXECUTIVE

Time Allotment: 6 hours

Time Allotment per Objective:

<b>1 hour</b>	<b>Objective I:</b>	Executives will understand the <i>National Criminal Intelligence Sharing Plan</i> (NCISP), <i>Information Sharing Environment Implementation Plan</i> (ISE IP), fusion center concept, and their own roles in each.
<b>1 hour</b>	<b>Objective II:</b>	Executives will understand the philosophy and practices of intelligence-led policing.
<b>2 hours</b>	<b>Objective III:</b>	Executives will understand the criminal intelligence process and its role in enhancing public safety.
<b>1 hour</b>	<b>Objective IV:</b>	Executives will understand the legal, privacy, and ethical issues relating to criminal intelligence.
<b>1 hour</b>	<b>Objective V:</b>	Executives will be provided with information on existing criminal information sharing networks and resources available in support of their agencies.

\*It is recommended that the most current developments in the field (e.g., fusion centers, *Information Sharing Environment* (ISE) *Implementation Plan* (IP), and updated terminology) be referenced in the curriculum for each training objective.

### SUMMARY

The intelligence function will not be successful without support from the agency's chief executive. Rather than knowing the processes of law enforcement intelligence, the chief executive needs to know what value the intelligence function will provide to the agency, the resources needed for the intelligence function to be effective, and the challenges—as well as potential liabilities—that are inherent in the intelligence process. Since many chief executives have minimal experience in contemporary law enforcement intelligence, they also need insight on new and changing roles and responsibilities of the intelligence function. For example, law enforcement executives will no doubt have some impression of fusion centers and the Information Sharing Environment, but they are not likely to have sufficient detailed information to understand the role of their agency in these new developments and the changes in law enforcement intelligence philosophy. The Minimum Criminal Intelligence Training Standards for Law Enforcement Executives are designed to address these needs.

**Objective I:** Executives will understand the *National Criminal Intelligence Sharing Plan* (NCISP), *Information Sharing Environment Implementation Plan* (ISE IP), fusion center concept, and their own roles in each.

1 hour	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Overview of the NCISP	<ul style="list-style-type: none"> <li>• <i>National Criminal Intelligence Sharing Plan</i></li> </ul>
	2. Impediments to information sharing	<ul style="list-style-type: none"> <li>• Community-oriented policing</li> </ul>
	3. Information sharing framework	<ul style="list-style-type: none"> <li>• Fusion centers, ISE IP, and local/regional initiatives</li> </ul>

**Objective II:** Executives will understand the philosophy and practices of intelligence-led policing.

1 hour	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Overview of the philosophy of intelligence-led policing	<ul style="list-style-type: none"> <li>• The intelligence function</li> <li>• Using intelligence to support and develop policy</li> <li>• Executive leadership roles and responsibilities</li> </ul>
	2. Overview of best practices in intelligence-led policing	<ul style="list-style-type: none"> <li>• Elements of:                             <ul style="list-style-type: none"> <li>• Community policing</li> <li>• Problem-oriented policing</li> <li>• CompStat</li> <li>• Other initiatives</li> </ul> </li> </ul>

**Objective III:** Executives will understand the criminal intelligence process and its role in enhancing public safety.

2 hours	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Why intelligence is important to the law enforcement executive	<ul style="list-style-type: none"> <li>• Types of intelligence (strategic/tactical)</li> <li>• Available products (briefs, reports/charts)</li> </ul>
	2. Intelligence process/cycle	<ul style="list-style-type: none"> <li>• Evaluating progress/performance</li> <li>• Demonstrate translation from intelligence to operational</li> </ul>
	3. Policies and procedures	<ul style="list-style-type: none"> <li>• Overview of the need for policies and procedures for intelligence officers and intelligence units</li> <li>• Provide glossary/common language as a handout</li> </ul>
	4. The following are recommended to be included in the curriculum, but not as specific standards	<ul style="list-style-type: none"> <li>• Impediments to the intelligence process/cycle</li> <li>• Building a successful intelligence unit</li> <li>• Managing/maximizing intelligence resources</li> </ul>

**Objective IV:** Executives will understand the legal, privacy, and ethical issues relating to criminal intelligence.

	Standards	Topics to Be Considered for Curriculum/Sources of Information
<b>1 hour</b>	1. Overview of legal and liability issues, intelligence audits/integrity, accountability, 28 CFR Part 23, and standards for protecting information	<ul style="list-style-type: none"> <li>• Provide model policy/guidelines as a handout</li> <li>• Possible resources include U.S. Attorneys' Offices, District Attorneys' Offices, and local prosecutors</li> </ul>
	2. Overview of community trust and communication with citizens and media (briefing city and community leaders on local ordinances)	<ul style="list-style-type: none"> <li>• Ethics</li> <li>• Public relations (handling difficult situations)</li> </ul>

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

	Standards	Topics to Be Considered for Curriculum/Sources of Information
<b>1 hour</b>	1. Sources of information/available resources	<ul style="list-style-type: none"> <li>• Law enforcement and intelligence systems</li> <li>• Open sources</li> <li>• Demonstration of selected systems</li> </ul>
	2. Overview of support materials	<ul style="list-style-type: none"> <li>• Resource guide, contacts, standards, etc.</li> </ul>
	3. Strategies to build relationships/networking	<ul style="list-style-type: none"> <li>• Discuss how intelligence is not only technical, it is a human effort</li> <li>• Provide information on associations/networking opportunities</li> </ul>
	4. Public/private partnerships	<ul style="list-style-type: none"> <li>• Networking and information sharing</li> </ul>



## GENERAL LAW ENFORCEMENT OFFICER— BASIC CRIMINAL INTELLIGENCE

Time Allotment: 2 hours

Time Allotment per Objective:

<b>40 minutes</b>	Objective I:	Law enforcement officers will understand the criminal intelligence process and its ability to enhance their contributions to the criminal justice system.
<b>10 minutes</b>	Objective II:	Law enforcement officers will be provided with information on available data systems, networks, and resources.
<b>40 minutes</b>	Objective III:	Law enforcement officers will be able to identify key signs of criminal activity and procedures for collecting data on and reporting such activity.
<b>30 minutes</b>	Objective IV:	Law enforcement officers will gain an understanding of the legal, privacy, and ethical limitations placed on the collection of criminal intelligence information.

\*It is recommended that the most current developments in the field (e.g., fusion centers, *Information Sharing Environment (ISE) Implementation Plan (IP)*, and updated terminology) be referenced in the curriculum for each training objective.

### SUMMARY

One of the more significant changes in law enforcement intelligence in the post-9/11 era deals with the philosophy of information sharing. Previously, a critical part of the intelligence philosophy was to maintain operations security of intelligence reports. Inherently, this also meant that information sharing was minimal. The line-level officer rarely saw intelligence reports. The current philosophy, however, is that information sharing must be maximized—as much information about threats should be placed in as many law enforcement hands as possible. The reason: The more personnel who have information about threats, the greater the likelihood of stopping or mitigating the threats. However, because of the sensitive nature of intelligence, the information must be shared in an “informed manner.” That is, general law enforcement officers must understand the difference between intelligence records and criminal records, how to handle intelligence reports, and how raw information must be shared with the intelligence function. They must also understand the critical nature of their role in the entire intelligence process. The Minimum Criminal Intelligence Training Standards are designed to incorporate these critical issues.

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

40 minutes	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Officers' roles and responsibilities in the intelligence process/cycle	<ul style="list-style-type: none"> <li>• Ensure that officers understand the steps of the intelligence cycle</li> <li>• Discuss impediments to the process</li> <li>• Provide a copy of the intelligence policy or model intelligence policy</li> <li>• Provide a glossary of intelligence terms</li> </ul>
	2. Types of intelligence (strategic, tactical)	<ul style="list-style-type: none"> <li>• Define "strategic intelligence"</li> <li>• Define "tactical intelligence"</li> <li>• Provide examples of products</li> </ul>
	3. Origins/history of intelligence	<ul style="list-style-type: none"> <li>• Overview of the NCISP</li> </ul>
	4. Importance of intelligence for the law enforcement officer	<ul style="list-style-type: none"> <li>• Provide case examples of why intelligence is important for the agency and community served</li> </ul>
	5. Community policing and its relationship to the intelligence function	<ul style="list-style-type: none"> <li>• Maintaining community relations</li> <li>• Define "community-led policing"</li> <li>• Relationship between intelligence-led policing and community-oriented policing</li> <li>• Case examples</li> </ul>
	6. Information sharing framework	<ul style="list-style-type: none"> <li>• Fusion centers, ISE IP, and local/regional initiatives</li> </ul>
	7. Sources of information/available resources	<ul style="list-style-type: none"> <li>• Law enforcement and intelligence systems</li> <li>• Open sources</li> <li>• Demonstration of selected systems</li> </ul>

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

10 minutes	Standard	Topics to Be Considered for Curriculum/Sources of Information
	1. Provide overview of the types of systems available	<ul style="list-style-type: none"> <li>• Explain the significance of different programs</li> <li>• Types of systems (pointer systems, intelligence systems, etc.)</li> <li>• Discuss systems unique to participants</li> <li>• Provide a list or summary of available resources and systems</li> </ul>

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

40 minutes	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Importance of recording and submitting raw information	<ul style="list-style-type: none"> <li>• Provide a copy of agency communication process/procedures</li> <li>• Case examples</li> </ul>
	2. Information collection methods, reporting procedures, and use of law enforcement sharing systems	<ul style="list-style-type: none"> <li>• Provide examples of the intelligence process and how it can be a success</li> <li>• Provide instruction for understanding current threats</li> <li>• Provide techniques to recognize and report behavior related to criminal threats (Include use of field interview cards.)</li> <li>• Provide information on local/state/regional/federal systems and networks</li> <li>• Provide information on resources local officers might use to collect information (including open sources)</li> <li>• Case examples, videos (as time allows)</li> </ul>
	3. Understanding terminology	<ul style="list-style-type: none"> <li>• Define “intelligence” – what is and what is not intelligence; provide examples of products</li> <li>• Define “intelligence-led policing”</li> <li>• Develop glossary in form of pocket guide</li> </ul>

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

30 minutes	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Ethics	<ul style="list-style-type: none"> <li>• Explain why ethics are pertinent to information handling</li> </ul>
	2. Legal basis, limitations, and liability issues	<ul style="list-style-type: none"> <li>• Use legal advisor, if available</li> <li>• Include current regulations and provide copies of key regulations</li> </ul>
	3. 28 CFR Part 23	<ul style="list-style-type: none"> <li>• General overview of 28 CFR Part 23</li> <li>• Provide copy of regulation</li> </ul>
4. Right to privacy and protection of personal liberties—current privacy initiatives/concerns	<ul style="list-style-type: none"> <li>• Include issues/examples regarding privacy</li> <li>• Video—immigrant interview contrasting rights in the United States and their country of origin, particularly the First and Fourth Amendment rights</li> </ul>	



## GENERAL LAW ENFORCEMENT OFFICER— CRIMINAL INTELLIGENCE REFRESHER

Time Allotment: 2 hours

Time Allotment per Objective:

<b>40 minutes</b>	<b>Objective I:</b>	Law enforcement officers will understand the criminal intelligence process and its ability to enhance their contributions to the criminal justice system.
<b>10 minutes</b>	<b>Objective II:</b>	Law enforcement officers will be provided with information on available data systems, networks, and resources.
<b>40 minutes</b>	<b>Objective III:</b>	Law enforcement officers will be able to identify key signs of criminal activity and procedures for collecting data on and reporting such activity.
<b>30 minutes</b>	<b>Objective IV:</b>	Law enforcement officers will gain an understanding of the legal, privacy, and ethical limitations placed on the collection of criminal intelligence information.

\*It is recommended that the most current developments in the field (e.g., fusion centers, *Information Sharing Environment (ISE) Implementation Plan (IP)*, and updated terminology) be referenced in the curriculum for each training objective.

### SUMMARY

One of the more significant changes in law enforcement intelligence in the post-9/11 era deals with the philosophy of information sharing. Previously, a critical part of the intelligence philosophy was to maintain operations security of intelligence reports. Inherently, this also meant that information sharing was minimal. The current philosophy, however, is that information sharing must be maximized—as much information about threats should be placed in as many law enforcement hands as possible. The reason: The more personnel who have information about threats, the greater the likelihood of stopping or mitigating the threats. However, because of the sensitive nature of intelligence, the information must be shared in an “informed manner.” That is, general law enforcement officers must continue to understand the difference between intelligence records and criminal records, how to handle intelligence reports, and how raw information must be shared with the intelligence function. They must also understand the critical nature of their role in the entire intelligence process. The Criminal Intelligence Refresher standards are designed to incorporate these critical issues. These standards serve to reinforce the importance of information collection and the officers’ role in the intelligence process.

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

40 minutes	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Officers' roles and responsibilities in the intelligence process/cycle	<ul style="list-style-type: none"> <li>• Ensure that officers understand the steps of the intelligence cycle</li> <li>• Discuss impediments to the process</li> <li>• Provide a copy of the agency intelligence policy or model intelligence policy</li> <li>• Provide a glossary of intelligence terms</li> </ul>
	2. Types of intelligence (strategic, tactical)	<ul style="list-style-type: none"> <li>• Define "strategic intelligence"</li> <li>• Define "tactical intelligence"</li> <li>• Provide examples of products</li> </ul>
	3. Origins/history of intelligence	<ul style="list-style-type: none"> <li>• Overview of the NCISP</li> </ul>
	4. Importance of intelligence for the law enforcement officer	<ul style="list-style-type: none"> <li>• Provide case examples of why intelligence is important for the agency and community served</li> </ul>
	5. Community policing and the criminal intelligence collection function	<ul style="list-style-type: none"> <li>• Maintaining community relations</li> <li>• Define "community-led policing"</li> <li>• Relationship between intelligence-led policing and community-oriented policing</li> <li>• Case examples</li> </ul>
	6. Information sharing framework	<ul style="list-style-type: none"> <li>• Fusion centers, ISE IP, and local/regional initiatives</li> </ul>

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

10 minutes	Standard	Topics to Be Considered for Curriculum/Sources of Information
	1. Provide overview of the types of systems available	<ul style="list-style-type: none"> <li>• Explain the significance of different programs</li> <li>• Types of systems (pointer systems, intelligence systems, etc.)</li> <li>• Discuss systems unique to participants</li> <li>• Provide list or summary of available resources and systems</li> </ul>

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

40 minutes	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Review importance of recording and submitting intelligence information	<ul style="list-style-type: none"> <li>• Provide a copy of agency communication processes/procedures</li> <li>• Case examples</li> </ul>
	2. Update on information collection methods, reporting procedures, and use of law enforcement sharing systems (RISS, HIDTA, LEO, ATAC, JTTF)	<ul style="list-style-type: none"> <li>• Provide techniques to recognize key intelligence and criminal activity</li> <li>• Include use of field interview cards</li> <li>• Provide examples of the intelligence process and how it can be a success</li> </ul>
	3. Review the identification of sources of information	<ul style="list-style-type: none"> <li>• Case examples, videos</li> <li>• Provide instruction in understanding current threats</li> <li>• Provide information on local/state/regional/federal systems and networks</li> <li>• Online resources</li> <li>• Public/commercial data</li> </ul>
	4. Review and update of terminology	<ul style="list-style-type: none"> <li>• Define “intelligence” – what is and what is not intelligence; provide examples of products</li> <li>• Define “intelligence-led policing”</li> <li>• Develop glossary in form of pocket guide</li> </ul>

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

30 minutes	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Ethics	<ul style="list-style-type: none"> <li>• Explain why ethics are pertinent to information handling</li> </ul>
	2. Update on legal basis, limitations, and liability issues	<ul style="list-style-type: none"> <li>• Use legal advisor, if available</li> <li>• Include current regulations and provide copies of key regulations</li> </ul>
	3. Update on 28 CFR Part 23	<ul style="list-style-type: none"> <li>• General overview of 28 CFR Part 23</li> <li>• Provide copy of regulation</li> </ul>
	4. Review right to privacy and protection of personal liberties—current privacy initiatives/concerns	<ul style="list-style-type: none"> <li>• Include issues/examples regarding privacy</li> <li>• Video—immigrant interview contrasting rights in the United States and their country of origin, particularly the First and Fourth Amendment rights</li> </ul>



## CRIMINAL INTELLIGENCE OFFICER

Time Allotment: 40 hours minimum

Time Allotment per Objective:

<b>5 hours</b>	<b>Objective I:</b>	Intelligence officers will understand the criminal intelligence process and their critical role in the process.
<b>6 hours</b>	<b>Objective II:</b>	Intelligence officers will understand the legal, ethical, and privacy issues surrounding criminal intelligence and their liability as intelligence information collectors.
<b>4 hours</b>	<b>Objective III:</b>	Intelligence officers will be provided with information on Internet resources, information sharing systems, networks, and other sources of information.
<b>6 hours</b>	<b>Objective IV:</b>	Intelligence officers will gain an understanding of the proper handling of criminal intelligence information, including file management and information evaluation.
<b>6 hours</b>	<b>Objective V:</b>	Intelligence officers will understand the processes of developing tactical and strategic products and experience the development of some products.
<b>5 hours</b>	<b>Objective VI:</b>	Intelligence officers will experience the development of criminal intelligence from information through the critical thinking/ inference development process.
<b>5 hours</b>	<b>Objective VII:</b>	Intelligence officers will understand the tasks of building and implementing collection plans.
<b>3 hours</b>	A 3-hour roundtable discussion is recommended.	

\*It is recommended that the most current developments in the field (e.g., fusion centers, *Information Sharing Environment (ISE) Implementation Plan (IP)*, and updated terminology) be referenced in the curriculum for each training objective.

### SUMMARY

For the law enforcement professional assigned as an intelligence officer, there are several critical issues that emerge: the lawful basis for collecting raw information for an intelligence inquiry, maintaining operational security of collected information, and the proper method of submitting collected information to ensure that it provides the information needed by an analyst. The issue of civil rights as well as the ability to distinguish between behaviors that are “unusual” and those “which have a criminal nexus beyond mere suspicion” are intricately tied together. The intelligence officer must, at a minimum, have a clear understanding of these issues. Finally, the intelligence officer must understand the concept of “intelligence requirements” in order to effectively perform this function.

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

5 hours	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Introduction to intelligence	<ul style="list-style-type: none"> <li>• Discuss the origin/history of intelligence</li> <li>• Provide a glossary of intelligence terms</li> <li>• Provide an overview of the NCISP</li> </ul>
	2. Intelligence officers' roles and responsibilities in the intelligence process/ cycle	<ul style="list-style-type: none"> <li>• Ensure that intelligence officers understand the steps of the intelligence cycle</li> <li>• Discuss impediments to the process</li> <li>• Provide a copy of the agency intelligence policy or model intelligence policy</li> </ul>
	3. Importance of intelligence for the intelligence officer	<ul style="list-style-type: none"> <li>• Provide case examples of why intelligence is important for the agency and community served</li> </ul>
	4. Community policing and its relationship to the intelligence function	<ul style="list-style-type: none"> <li>• Maintaining community relations</li> <li>• Define "community-led policing"</li> <li>• Relationship between intelligence-led policing and community-oriented policing</li> <li>• Case examples</li> </ul>
	5. Networking	<ul style="list-style-type: none"> <li>• Liaise with peers, other agencies, organizations, and professional memberships for dissemination of information</li> <li>• Allow participants to discuss the way their agency networks</li> </ul>
	6. Information sharing framework	<ul style="list-style-type: none"> <li>• Fusion centers, ISE IP, and local/regional initiatives</li> </ul>

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

6 hours	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Legal basis and limitations	<ul style="list-style-type: none"> <li>• Use legal advisor, if available</li> <li>• Include current regulations and provide copies of key regulations, as appropriate</li> <li>• Possible resources include U.S. Attorneys' Offices, District Attorneys' Offices, and local prosecutors</li> </ul>
	2. 28 CFR Part 23	<ul style="list-style-type: none"> <li>• General overview of 28 CFR Part 23</li> <li>• Provide copy of regulation</li> </ul>
	3. Privacy, civil liberties, and civil rights	<ul style="list-style-type: none"> <li>• Include issues/examples regarding privacy</li> <li>• Video—immigrant interview contrasting rights in the United States and their country of origin, particularly the First and Fourth Amendment rights</li> </ul>
	4. Ethics	<ul style="list-style-type: none"> <li>• Explain why ethics are pertinent to information handling</li> <li>• Provide scenario to illustrate importance</li> </ul>
	5. Civil liability	<ul style="list-style-type: none"> <li>• Provide an overview of liability issues in the intelligence process</li> </ul>

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

4 hours	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Sources of information/available resources	<ul style="list-style-type: none"> <li>• Law enforcement and intelligence information systems, such as RISS, HSIN, and LEO</li> <li>• Open source information</li> <li>• Demonstration of selected systems</li> <li>• Human source development</li> </ul>
2. Research methods	<ul style="list-style-type: none"> <li>• Research methods versus investigative methods</li> </ul>	

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

6 hours	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Handling evidence/intelligence	
	2. Markings and confidential information	<ul style="list-style-type: none"> <li>• Classified</li> <li>• Sensitive But Unclassified (SBU)</li> <li>• Controlled Unclassified Information (CUI)</li> <li>• State-authorized markings</li> </ul>
	3. Operational security processes	<ul style="list-style-type: none"> <li>• Protecting methods and sources</li> <li>• Policies/rules</li> <li>• Disclosure of sensitive information to media, other law enforcement entities, citizens, public safety agencies, etc.</li> </ul>
	4. Information management	<ul style="list-style-type: none"> <li>• Electronic</li> <li>• Archives (storage)</li> <li>• Files (hard copy)</li> </ul>
	5. Evaluation	<ul style="list-style-type: none"> <li>• Reliability/source validity</li> </ul>
	6. Courtroom testimony	<ul style="list-style-type: none"> <li>• Include short role-playing session</li> <li>• Provide “dos” and “don’ts”</li> </ul>
	7. Marking and using confidential information	<ul style="list-style-type: none"> <li>• Classified</li> <li>• Sensitive But Unclassified (SBU)</li> <li>• Proposed CUI framework</li> <li>• State-authorized markings</li> </ul>

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

6 hours	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Types of intelligence products	
	2. Principles of good report writing	<ul style="list-style-type: none"> <li>• Provide differences between intelligence/ investigative projects/reports, briefs, etc.</li> </ul>
	3. Uses of intelligence products	<ul style="list-style-type: none"> <li>• Strategic, tactical, operational, data visualization, and value of products</li> <li>• Threat assessments</li> </ul>
	4. Feedback	<ul style="list-style-type: none"> <li>• Does the intelligence product meet the needs of its intended purpose?</li> </ul>

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

5 hours	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Critical thinking	
	2. Logic/fallacies of logic	<ul style="list-style-type: none"> <li>• Analysis of competing hypotheses</li> </ul>
	3. Inference developments	
	4. Recommendations development	
	5. Crime indicators	

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

5 hours	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Developing collection and investigative plans	<ul style="list-style-type: none"> <li>• Class exercise—develop a collection plan</li> <li>• Matching intelligence collection strategies to requirements</li> </ul>
	2. Needs of the consumer	<ul style="list-style-type: none"> <li>• Does the information meet the needs of its intended purpose?</li> </ul>
	3. Infusing consumer feedback into the intelligence cycle	

\*A three-hour roundtable discussion is recommended as part of this 40-hour training.



## TRAIN-THE-TRAINER

Time Allotment: 16 hours minimum

Time Allotment per Objective:

<b>2 hours</b>	<b>Objective I:</b>	Trainers will understand the intelligence process and how it functions.
<b>1 hour</b>	<b>Objective II:</b>	Trainers will understand the <i>National Criminal Intelligence Sharing Plan</i> (NCISP), intelligence-led policing, and other national information sharing initiatives and the role they play in reducing crime and violence throughout the country.
<b>5 hours</b>	<b>Objective III:</b>	Trainers will be provided with information regarding intelligence systems; other sources of information; current criminal threats, trends, and patterns; and strategies to access and apply information.
<b>2 hours</b>	<b>Objective IV:</b>	Trainers will understand the processes and uses of tactical and strategic intelligence products.
<b>3 hours</b>	<b>Objective V:</b>	Trainers will be familiar with the latest innovations in training and will be aware of appropriate topical resources for criminal intelligence instruction.
<b>1 hour</b>	<b>Objective VI:</b>	Trainers will be knowledgeable of existing course materials and their use.
<b>1 hour</b>	<b>Objective VII:</b>	Trainers will be aware of the legal, privacy, and ethical issues relating to intelligence.
<b>1 hour</b>	<b>Objective VIII:</b>	Trainers will prepare and present a short module on intelligence.

\*It is recommended that the most current developments in the field (e.g., fusion centers, *Information Sharing Environment* (ISE) *Implementation Plan* (IP), and updated terminology) be referenced in the curriculum for each training objective.

### SUMMARY

The NCISP states that all law enforcement officers should have training on the criminal intelligence process. The intent of this training is to ensure that an agency may effectively develop an intelligence capacity and participate in the Information Sharing Environment. One of the most efficient ways to provide widespread intelligence awareness training to America's police officers is through a Train-the-Trainer program. The intent of a Train-the-Trainer program is that an agency would send personnel to this program in order to receive the knowledge and curricula needed to develop the necessary foundation of information on intelligence processes required so that an effective intelligence capacity could be built into an agency. The Minimum Criminal Intelligence Training Standards for a Train-the-Trainer program are designed to ensure that the critical information needed for the new trainer is incorporated into the curriculum.

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

2 hours	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Intelligence process/cycle	<ul style="list-style-type: none"> <li>• Ensure that trainers fully understand and can apply the steps of the intelligence cycle</li> <li>• Include the roles and responsibilities of intelligence personnel</li> <li>• Impediments to the process</li> <li>• Case examples; videos</li> </ul>
	2. Origin/history of intelligence	
	3. Why intelligence is important	<ul style="list-style-type: none"> <li>• Provide examples of why intelligence is important to different people/groups—executives, policymakers, investigators, analysts, etc.</li> <li>• Case examples</li> </ul>

**Objective II:** Trainers will understand the *National Criminal Intelligence Sharing Plan* (NCISP), intelligence-led policing, and other national information sharing initiatives and the role they play in reducing crime and violence throughout the country.

1 hour	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Overview of the <i>National Criminal Intelligence Sharing Plan</i> (NCISP) and information sharing initiatives and systems	<ul style="list-style-type: none"> <li>• Information sharing/information sharing initiatives (LEISP, Global, N-DEx) (Curriculum developers should include current initiatives and those of local and/or regional importance.)</li> <li>• Threats facing community, state, nation</li> <li>• Terrorism/topical materials</li> <li>• Intelligence-led policing</li> <li>• Community policing</li> </ul>
	2. Information sharing framework	<ul style="list-style-type: none"> <li>• Fusion centers, ISE IP, and local/regional initiatives</li> </ul>
	3. Intelligence-led policing, community policing, and their relationship to intelligence	<ul style="list-style-type: none"> <li>• Define “intelligence-led policing”</li> <li>• Discuss benefits of intelligence-led policing</li> </ul>

**Objective III:** Trainers will be provided with information regarding intelligence systems; other sources of information; current criminal threats, trends, and patterns; and strategies to access and apply information.

5 hours	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Intelligence sharing systems	<ul style="list-style-type: none"> <li>• Law enforcement and intelligence information systems</li> <li>• Open source information (inclusive of criminal history, RISS)</li> <li>• Demonstration of selected systems</li> </ul>
2. Applying intelligence to current threats	<ul style="list-style-type: none"> <li>• Motives, methods, targets</li> </ul>	

**Objective IV:** Trainers will understand the processes and uses of tactical and strategic intelligence products.

2 hours	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Understanding terminology	<ul style="list-style-type: none"> <li>• Define “intelligence” – what is and what is not intelligence; provide examples of products</li> <li>• Define “intelligence-led policing”</li> <li>• Develop glossary in form of pocket guide</li> </ul>
	2. Types of intelligence	<ul style="list-style-type: none"> <li>• Define “strategic intelligence”</li> <li>• Define “tactical intelligence”</li> <li>• Provide examples of products</li> </ul>
3. Intelligence products (intelligence reports, data/link analysis, etc.)	<ul style="list-style-type: none"> <li>• Understanding reports, differences between strategic and tactical intelligence</li> </ul>	

**Objective V:** Trainers will be familiar with the latest innovations in training and will be aware of appropriate topical resources for criminal intelligence instruction.

3 hours	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Current innovations and instructional techniques	
2. Audiovisual aids, instructional media, and their use	<ul style="list-style-type: none"> <li>• Familiarity with a variety of audiovisual aids</li> <li>• Troubleshooting technical issues</li> <li>• Training materials package</li> </ul>	

**Objective VI:** Trainers will be knowledgeable of existing course materials and their use.

1 hour	Standard	Topics to Be Considered for Curriculum/Sources of Information
	1. Familiarity with existing curricula, lesson plans, tests, and exercises	<ul style="list-style-type: none"> <li>• Handouts with lesson plans, materials, and exercise demonstrations</li> <li>• Understand what types of training are offered and by whom</li> </ul>

**Objective VII:** Trainers will be aware of the legal, privacy, and ethical issues relating to intelligence.

1 hour	Standards	Topics to Be Considered for Curriculum/Sources of Information
	1. Legal basis and limitations	<ul style="list-style-type: none"> <li>• Current regulations and how they apply to intelligence</li> <li>• Intelligence audits/integrity</li> </ul>
	2. Liability issues	<ul style="list-style-type: none"> <li>• Standards for protecting information</li> </ul>
	3. 28 CFR Part 23	<ul style="list-style-type: none"> <li>• Provide copy of regulation</li> </ul>
	4. Right to privacy and protection of personal liberties (examples of privacy issues/ initiatives)	<ul style="list-style-type: none"> <li>• Provide scenarios illustrating privacy issues</li> <li>• Discuss strategy to protect personal information</li> </ul>
	5. Ethics	

**Objective VIII:** Trainers will prepare and present a short module on intelligence.

1 hour	Standard	Topics to Be Considered for Curriculum/Sources of Information
	1. Trainers will provide participants with topics or allow students to choose topics for presentation. Participants may use multimedia. The length of the presentation is dependent on the number of participants and remaining time available.	

## APPENDIX

### CRIMINAL INTELLIGENCE GLOSSARY OF TERMS—OCTOBER 2007

Law enforcement agencies at all levels are working together more than ever to support information sharing. It is important to note that there is a tremendous effort under way to streamline intelligence terms to facilitate information sharing. As a result, criminal intelligence terminology is changing. It is recommended that organizations stay abreast of emerging intelligence-related terminology.

The definitions contained herein are provided from the perspective of criminal intelligence. Further, it is recognized that some words and phrases will have alternate or additional meanings when used in the context of national security intelligence, the military, or business. The definitions are intended to be merely descriptive of an entity, issue, or process that may be encountered by those working with the criminal intelligence function. Definitions may differ according to state statutes or local rules.

#### **Access (to sensitive information)**

Sensitive information and/or intelligence may be released by a law enforcement agency when at least one of the following four prescribed circumstances applies to the person(s) receiving the information:

##### *Right to Know*

Based on having legal authority, one's official position, legal mandates, or official agreements, allowing the individual to receive intelligence reports.

##### *Need to Know*

As a result of jurisdictional, organizational, or operational necessities, intelligence or information is disseminated to further an investigation.

##### *Investigatory Value*

Intelligence or information is disseminated in the law enforcement community for surveillance, apprehension, or furtherance of an investigation.

##### *Public Value*

Intelligence or information can be released to the public when there is a need to know and a right to know the information because of the value that may be derived from public dissemination to (1) aid in locating targets/suspects and (2) for public safety purposes (i.e., hardening targets, taking precautions).

#### **Actionable**

Intelligence and information with sufficient specificity and detail to implement explicit responses to prevent a crime or terrorist attack.

#### **Administrative Analysis**

The analysis of economic, geographic, demographic, census, or behavioral data to identify trends and conditions useful to aid administrators in making policy and/or resource allocation decisions.

#### **Allocation**

Collection and analysis of information that shows relationships among varied individuals suspected of being involved in criminal activity that may provide insight into the criminal operation and which investigative strategies might work best.

#### **Analysis**

That activity whereby meaning, actual or suggested, is derived through organizing and systematically examining diverse information and applying inductive or deductive logic for the purposes of criminal investigation or assessment.

#### **Archiving (Records)**

The maintenance of records in remote storage after a case has been closed or disposed of, as a matter of contingency, should the records be needed for later reference.

#### **Association Analysis**

The entry of critical investigative and/or assessment variables into a two-axis matrix to examine the relationships and patterns that emerge as the variables are correlated in the matrix.

## **Automated Trusted Information Exchange (ATIX)**

Operated by the Regional Information Sharing Systems®, ATIX is a secure means to disseminate national security or terrorist threat information to law enforcement and other first responders via the ATIX electronic bulletin board, secure Web site, and secure e-mail.

## **Bias/Hate Crime**

Any criminal act directed toward any person or group as a result of that person's race, ethnicity, religious affiliation, or sexual preference.

## **C3**

An intelligence application concept initially used by military intelligence that stands for command, control, and communication as the hallmark for effective intelligence operations.

## **Clandestine Activity**

An activity that is usually extensive and goal-oriented, planned, and executed to conceal the existence of the operation. Only participants and the agency sponsoring the activity are intended to know about the operation. "Storefront" operations, "stings," and certain concentrated undercover investigations (such as ABSCAM) can be classified as clandestine collections.

## **Classified Information/Intelligence**

A uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism, to ensure that certain information is maintained in confidence in order to protect citizens, U.S. democratic institutions, U.S. homeland security, and U.S. interactions with foreign nations and entities.

### *Top Secret Classification*

Applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe (Executive Order 12958, March 25, 2003).

### *Secret Classification*

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

that the original classification authority is able to identify or describe (Executive Order 12958, March 25, 2003).

### *Confidential Classification*

Applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe (Executive Order 12958, March 25, 2003).

## **Collation (of information)**

A review of collected and evaluated information to determine its substantive applicability to a case or problem at issue and placement of useful information into a form or system that permits easy and rapid access and retrieval.

## **Collection (of information)**

The identification, location, and recording/storing of information, typically from an original source and using both human and technological means, for input into the intelligence cycle for the purpose of meeting a defined tactical or strategic intelligence goal.

## **Collection Plan**

The preliminary step toward completing an assessment of intelligence requirements to determine what type of information needs to be collected, alternatives for how to collect the information, and a timeline for collecting the information.

## **Command and Control**

Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of a mission.

## **Commodity (Illegal)**

Any item or substance that is inherently unlawful to possess (contraband) or materials which, if not contraband, are themselves being distributed, transacted, or marketed in an unlawful manner.

## **Commodity Flow Analysis**

Graphic depictions and descriptions of transactions, shipment, and distribution of contraband goods and

money derived from unlawful activities in order to aid in the disruption of the unlawful activities and apprehend those persons involved in all aspects of the unlawful activities.

## **Communications Intelligence (COMINT)**

The capture of information, either encrypted or in "plaintext," exchanged between intelligence targets or transmitted by a known or suspected intelligence target for the purposes of tracking communications patterns and protocols (traffic analysis), establishing links between intercommunicating parties or groups, and/or analysis of the substantive meaning of the communication.

## **Conclusion**

A definitive statement about a suspect, action, or state of nature based on the analysis of information.

## **Confidential**

See Classified Information/Intelligence, Confidential Classification.

## **Continuing Criminal Enterprise**

Any individual, partnership, corporation, association, or other legal entity and any union or group of individuals associated in fact, although not a legal entity, that are involved in a continuing or perpetuating criminal activity.

## **Controlled Unclassified Information (CUI)**

This is a proposed term to replace the term "Sensitive But Unclassified." It has not been officially adopted.

## **Coordination**

The process of interrelating work functions, responsibilities, duties, resources, and initiatives directed toward goal attainment.

## **Counterintelligence**

Information compiled, analyzed, and/or disseminated in an effort to investigate espionage, sedition, or subversion that is related to national security concerns. A national security intelligence activity that involves blocking or developing a strategic response to other groups, governments,

or individuals through the identification, neutralization, and manipulation of their intelligence services.

## **Covert Intelligence**

A covert activity is planned and executed to conceal the collection of information and/or the identity of any officer or agent participating in the activity.

## **Crime Analysis**

The process of analyzing information collected on crimes and police service delivery variables in order to give direction for police officer deployment, resource allocation, and policing strategies as a means to maximize crime prevention activities and the cost-effective operation of the police department.

## **Crime-Pattern Analysis**

An assessment of the nature, extent, and changes of crime based on the characteristics of the criminal incident, including modus operandi, temporal, and geographic variables.

## **Criminal History Record Information (CHRI)**

Information collected by criminal justice agencies on individuals, consisting of identifiable descriptions and notations of arrests, detentions, indictments, information, or other formal criminal charges and any disposition arising therefrom, including sentencing, correctional supervision, and/or release. The term does not include identification information, such as fingerprint records, to the extent that such information does not indicate involvement of the individual in the criminal justice system.

## **Criminal Informant**

See Informant.

## **Criminal Intelligence**

See Intelligence (Criminal) and Law Enforcement Intelligence.

## **Criminal Investigative Analysis**

An analytic process that studies serial offenders, victims, and crime scenes in order to assess characteristics and behaviors of offender(s) with the intent to identify or aid in the identification of the offender(s).

## **Criminal Predicate**

Information about an individual or his/her behavior that may be collected and stored in a law enforcement intelligence records system only when there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.

## **Cryptanalysis**

The process of deciphering encrypted communications of an intelligence target.

## **Cryptography**

The creation of a communications code/encryption system for communication transmission with the intent of precluding the consumption and interpretation of one's own messages.

## **Cryptology**

The study of communications encryption methods that deal with the development of "codes" and the "scrambling" of communications in order to prevent the interception of the communications by an unauthorized or unintended party.

## **Data Element**

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

## **Data Owner**

The agency that originally enters information or data into a law enforcement records system.

## **Data Quality**

Controls implemented to ensure that all information in a law enforcement agency's records system is complete, accurate, and secure.

## **Deconfliction**

The process or system that is used to determine whether multiple law enforcement agencies are investigating the same person or crime and that provides notification to each agency involved of the shared interest in the case, as well as providing contact information. This is an information and intelligence sharing process that seeks to minimize conflicts between agencies and maximize the effectiveness of an investigation.

## **Deductive Logic**

The reasoning process of taking information and arriving at conclusions from within that information.

## **Deployment**

The short-term assignment of personnel to address specific crime problems or police service demands.

## **Designated State and/or Major Urban Area Fusion Center**

The fusion center in each state designated as the primary or lead fusion center for the information sharing environment.

## **Dissemination (of Intelligence)**

The process of effectively distributing analyzed intelligence utilizing certain protocols in the most appropriate format to those in need of the information to facilitate their accomplishment of organizational goals.

## **Due Process**

Fundamental fairness during the course of the criminal justice process, including adherence to legal standards and the civil rights of the police constituency; the adherence to principles that are fundamental to justice.

## **El Paso Intelligence Center (EPIC)**

A cooperative intelligence center serving as a clearinghouse and intelligence resource for local, state, and federal law enforcement agencies. Its primary concern is drug trafficking; however, intelligence on other crimes is also managed by EPIC.

## **Enterprise**

Any individual, partnership, corporation, association, or other legal entity and any union or group of individuals associated in fact, although not a legal entity.

## **Estimate**

See Intelligence Estimate.

## **Evaluation (of Information)**

All information collected for the intelligence cycle is reviewed for its quality with an assessment of the validity and reliability of the information.

### **Event Flow Analysis**

Graphic depictions and descriptions of incidents, behaviors, and people involved in an unlawful event, intended to help understand how an event occurred as a tool to aid in prosecution as well as prevention of future unlawful events.

### **Exemptions (to the Freedom of Information Act)**

Circumstances wherein a law enforcement agency is not required to disclose information from a Freedom of Information Act (FOIA) request.

### **Field Intelligence Group (FIG)**

The centralized intelligence component in a Federal Bureau of Investigation (FBI) field office that is responsible for the management, execution, and coordination of intelligence functions within the field office region.

### **Field Intelligence Report (FIR)**

An officer-initiated interview of a person believed by the officer to be acting in a suspicious manner that may be indicative of planning or preparing to conduct criminal activity.

### **Financial Analysis**

A review and analysis of financial data to ascertain the presence of criminal activity. It can include bank record analysis, net worth analysis, financial profiles, source and applications of funds, financial statement analysis, and/or Bank Secrecy Act record analysis. It can also show destinations of proceeds of crime and support prosecutions.

### **Flow Analysis**

The review of raw data to determine the sequence of events or interactions that may reflect criminal activity. Flow analysis includes timelines, event flow analysis, commodity flow analysis, and activity flow analysis and may show missing actions or events that need further investigation.

### **For Official Use Only (FOUO)**

A designation applied to unclassified sensitive information that may be exempt from mandatory release to the public under the FOIA.

### **Forecast (as related to Criminal Intelligence)**

The product of an analytic process that provides a probability of future crimes and crime patterns based on a comprehensive, integrated analysis of past, current, and developing trends.

### **Freedom of Information Act (FOIA)**

The Freedom of Information Act, 5 U.S.C. 552, enacted in 1966, statutorily provides that any person has a right, enforceable in court, to access federal agency records, except to the extent that such records (or portions thereof) are protected from disclosure by one of nine exemptions.

### **Fusion Center**

The physical location of the law enforcement intelligence fusion process.

### ***Fusion Center Guidelines***

A series of nationally recognized standards developed by law enforcement intelligence subject-matter experts designed for the good practice of developing and managing an intelligence fusion center.

### **Fusion Process**

The overarching process of managing the flow of information and intelligence across levels and sectors of government.

### **Granularity**

Considers the specific details and pieces of information, including nuances and situational inferences, that constitute the elements on which intelligence is developed through analysis.

### **Guidelines**

See Intelligence Records Guidelines.

### **Homeland Security Advisory System**

An information and communications structure designed by the U.S. government for disseminating information to all levels of government and the American people regarding the risk of terrorist attacks and for providing a framework to assess the risk at five levels: Low, Guarded, Elevated, High, and Severe.

## **Human Intelligence (HUMINT)**

Intelligence-gathering methods that require human interaction or observation of the target or targeted environment. The intelligence is collected through the use of one's direct senses or the optical and/or audio enhancement of the senses.

## **Hypothesis (from Criminal Intelligence Analysis)**

An interim conclusion regarding persons, events, and/or commodities based on the accumulation and analysis of intelligence information that is to be proved or disproved by further investigation and analysis.

## **Imagery**

The representation of an object or locale produced on any medium by optical or electronic means. The nature of the image will be dependent on the sensing media and sensing platform.

## **Indicator**

Generally defined and observable actions that, based on an analysis of past known behaviors and characteristics, collectively suggest that a person may be committing, may be preparing to commit, or has committed an unlawful act.

## **Inductive Logic**

The reasoning process of taking diverse pieces of specific information and inferring a broader meaning of the information through the course of hypothesis development.

## **Inference Development**

The creation of a probabilistic conclusion, estimate, or prediction related to an intelligence target based on the use of inductive or deductive logic in the analysis of raw information related to the target.

## **Informant**

An individual not affiliated with a law enforcement agency who provides information about criminal behavior to a law enforcement agency. An informant may be a community member, a businessperson, or a criminal informant who seeks to protect himself/herself from prosecution and/or provide the information in exchange for payment.

## **Information**

Pieces of raw, unanalyzed data that identify persons, evidence, or events or illustrate processes that indicate the incidence of a criminal event or witnesses or evidence of a criminal event.

## **Information Classification**

See Classified Information/Intelligence.

## **Information Evaluation**

See Evaluation (of Information).

## **Information Sharing Environment**

A trusted partnership among all levels of government, the private sector, and foreign partners to detect, prevent, preempt, and mitigate the effects of terrorism against territory, people, and interests of the United States of America. This partnership enables the trusted, secure, and appropriate exchange of terrorism information, in the first instance, across the five federal communities; to and from state, local, and tribal governments, foreign allies, and the private sector; and at all levels of security classifications.

## **Information Sharing System**

An integrated and secure methodology, whether computerized or manual, designed to efficiently and effectively distribute critical information about offenders, crimes, and/or events in order to enhance prevention and apprehension activities by law enforcement.

## **Information System**

An organized means, whether manual or electronic, of collecting, processing, storing, and retrieving information on individual entities for purposes of record and reference.

## **Intelligence (Criminal)**

The product of the analysis of raw information related to crimes or crime patterns with respect to an identifiable person or group of persons in an effort to anticipate, prevent, or monitor possible criminal activity.

## **Intelligence Analyst**

A professional position in which the incumbent is responsible for taking the varied facts, documentation of circumstances, evidence, interviews, and any other material related to a

crime and organizing them into a logical and related framework for the purposes of developing a criminal case, explaining a criminal phenomenon, describing crime and crime trends and/or preparing materials for court and prosecution, or arriving at an assessment of a crime problem or crime group.

### **Intelligence Assessment**

A comprehensive report on an intelligence issue related to criminal or national security threats available to local, state, tribal, and federal law enforcement agencies.

### **Intelligence Bulletins**

A finished intelligence product in article format that describes new developments and evolving trends. The bulletins are typically Sensitive But Unclassified (SBU) and available for distribution to local, state, tribal, and federal law enforcement.

### **Intelligence Community**

Those agencies of the U.S. government, including the military, that have the responsibility of preventing breeches to U.S. national security and responding to national security threats.

### **Intelligence Cycle**

An organized process by which information is gathered, assessed, and distributed in order to fulfill the goals of the intelligence function. It is a method of performing analytic activities and placing the analysis in a useable form.

### **Intelligence Estimate**

The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to criminal offenders and terrorists and the order of probability of their adoption. Includes strategic projections on the economic, human, and/or quantitative criminal impact of the crime or issue that is subject to analysis.

### **Intelligence Function**

That activity within a law enforcement agency responsible for some aspect of law enforcement intelligence, whether collection, analysis, and/or dissemination.

### **Intelligence Gap**

An unanswered question about a cyber, criminal, or national security issue or threat.

### **Intelligence Information Reports (IIR)**

Raw, unevaluated intelligence concerning “perishable” or time-limited information about criminal or national security issues. Although the full IIR may be classified, local, state, and tribal law enforcement agencies will have access to Sensitive But Unclassified information in the report under the tear line.

### **Intelligence-Led Policing**

The dynamic use of intelligence to guide operational law enforcement activities to targets, commodities, or threats for both tactical responses and strategic decision making for resource allocation and/or strategic responses.

### **Intelligence Mission**

The role that the intelligence function of a law enforcement agency fulfills in support of the overall mission of the agency; it specifies in general language what the function is intended to accomplish.

### **Intelligence Mutual Aid Pact (IMAP)**

A formal agreement between law enforcement agencies designed to expedite the process of sharing information in intelligence records.

### **Intelligence Officer**

A law enforcement officer assigned to an agency’s intelligence function for purposes of investigation, liaison, or other intelligence-related activity that requires or benefits from having a sworn officer perform the activity.

### **Intelligence Products**

Reports or documents that contain assessments, forecasts, associations, links, and other outputs from the analytic process that may be disseminated for use by law enforcement agencies for prevention of crimes, target hardening, apprehension of offenders, and prosecution.

## **Intelligence Records (Files)**

Stored information on the activities and associations of individuals, organizations, businesses, and groups who are suspected (reasonable suspicion) of being involved in the actual or attempted planning, organizing, financing, or commissioning of criminal acts or are suspected of being or having been involved in criminal activities with known or suspected crime figures.

## **Intelligence Records Guidelines**

Derived from the federal regulation 28 CFR Part 23, these are guidelines/standards for the development of records management policies and procedures used by law enforcement agencies.

## **International Criminal Police Organization (INTERPOL)**

INTERPOL is a worldwide law enforcement organization established for mutual assistance in the prevention, detection, and deterrence of international crimes. It houses international police databases, provides secure international communications between member countries for the exchange of routine criminal investigative information, and is an information clearinghouse on international criminals/fugitives and stolen properties.

## **Key Word In Context (KWIC)**

An automated system that indexes selected key words that represent the evidence or information being stored.

## **Law Enforcement Intelligence**

The end product (output) of an analytic process that collects and assesses information about crimes and/or criminal enterprises with the purpose of making judgments and inferences about community conditions, potential problems, and criminal activity with the intent to pursue criminal prosecution, project crime trends, or support informed decision making by management.

## **Law Enforcement Sensitive (LES)**

Sensitive But Unclassified information specifically compiled for law enforcement purposes that, if not protected from unauthorized access, could reasonably be expected to 1) interfere with law enforcement proceedings, 2) deprive a person of a right to a fair trial or impartial adjudication,

3) constitute an unwarranted invasion of the personal privacy of others, 4) disclose the identity of a confidential source, 5) disclose investigative techniques and procedures, and/or 6) endanger the life or physical safety of an individual.

## **Methods**

These are the methodologies (e.g., electronic surveillance or undercover operations) of how critical information is obtained and recorded.

## **Micro-Intelligence**

Intelligence activities focusing on current problems and crimes for either case development or resource allocation.

## **Money Laundering**

The practice of using multiple unlawful transactions of money and/or negotiable instruments gained through illegal activities with the intent of hiding the origin of the income, those who have been "paid" from the income, and/or the location of the unlawful income.

## **National Central Bureau (NCB or USNCB)**

The United States headquarters of INTERPOL is located in Washington, DC.

## **National Criminal Intelligence Resource Center (NCIRC)**

An Internet Web site that contains information regarding law enforcement intelligence operations and practices and provides criminal justice professionals with a centralized resource information bank to access a multitude of criminal intelligence resources to help law enforcement agencies develop, implement, and retain a lawful and effective intelligence capacity.

## **National Criminal Intelligence Sharing Plan (NCISP)**

A formal intelligence sharing initiative, supported by the U.S. Department of Justice, Office of Justice Programs, that securely links local, state, tribal, and federal law enforcement agencies, facilitating the exchange of critical intelligence information. The Plan contains model policies and standards and is a blueprint for law enforcement administrators to follow when enhancing or building an

intelligence function. It describes a nationwide communications capability that will link all levels of law enforcement personnel, including officers on the street, intelligence analysts, unit commanders, and police executives.

### **National Security Intelligence**

The collection and analysis of information concerned with the relationship and equilibrium of the United States with foreign powers, organizations, and persons with regard to political and economic factors, as well as the maintenance of the United States' sovereign principles.

### **Network**

A structure of interconnecting components designed to communicate with each other and perform a function or functions as a unit in a specified manner.

### **Open Communications (OPCOM)**

The collection of open or publicly available communications, broadcasts, audio or video recordings, propaganda, published statements, and other distributed written or recorded material for purposes of analyzing the information.

### **Open Source Information (or Intelligence)**

Individual data, records, reports, and assessments that may shed light on an investigatory target or event that do not require any legal process or any type of clandestine collection techniques for a law enforcement agency to obtain. Rather, it is obtained through means that meet copyright and commercial requirements of vendors, as well as being free of legal restrictions to access by anyone who seeks that information.

### **Operational Analysis**

An assessment of the methodology of a criminal enterprise or terrorist organization that depicts how the enterprise performs its activities, including communications, philosophy, compensation, security, and other variables that are essential for the enterprise to exist.

### **Operational Intelligence**

Information is evaluated and systematically organized on an active or potential target, such as

groups of or individual criminals, relevant premises, contact points, and methods of communication. This process is developmental in nature, wherein there are sufficient articulated reasons to suspect criminal activity. Intelligence activities explore the basis of those reasons and newly developed information in order to develop a case for arrest or indictment.

### **Outcome Evaluation**

The process of determining the value or amount of success in achieving a predetermined objective through defining the objective in some qualitative or quantitative measurable terms, identifying the proper criteria (or variables) to be used in measuring the success toward attaining the objective, determination and explanation of the degree of success, and recommendations for further program actions to attain the desired objectives/outcomes.

### **Planning**

The preparation for future situations, estimating organizational demands and resources needed to attend to those situations, and initiating strategies to respond to those situations.

### **Pointer System or Index**

A system that stores information designed to identify individuals, organizations, and/or crime methodologies with the purpose of linking law enforcement agencies that have similar investigative and/or intelligence interests in the entity defined by the system.

### **Policy**

The principles and values that guide the performance of a duty. A policy is not a statement of what must be done in a particular situation. Rather, it is a statement of guiding principles that should be followed in activities that are directed toward the attainment of goals.

### **Prediction**

The projection of future criminal actions or changes in the nature of crime trends or a criminal enterprise based on an analysis of information depicting historical trends from which a forecast is based.

### **Preventive Intelligence**

Intelligence that can be used to interdict or forestall a crime or terrorist attack.

## **Privacy (Information)**

The assurance that legal and constitutional restrictions on the collection, maintenance, use, and disclosure of personally identifiable information will be adhered to by criminal justice agencies, with use of such information to be strictly limited to circumstances in which legal process permits use of the personally identifiable information.

## **Privacy (Personal)**

The assurance that legal and constitutional restrictions on the collection, maintenance, use, and disclosure of behaviors of an individual—including his/her communications, associations, and transactions—will be adhered to by criminal justice agencies, with use of such information to be strictly limited to circumstances in which legal process authorizes surveillance and investigation.

## **Privacy Act**

Legislation that allows an individual to review almost all federal files (and state files under the auspices of the respective state privacy acts) pertaining to him/her, places restrictions on the disclosure of personally identifiable information, specifies that there be no secret records systems on individuals, and compels the government to reveal its information sources.

## **Proactive**

Taking action that is anticipatory to a problem or situation with the intent to eliminate or mitigate the effect of the incident.

## **Procedural Due Process**

Mandates and guarantees of law that ensure that the procedures employed during the course of the criminal justice process to deprive a person of life, liberty, or property meet constitutional standards.

## **Procedure**

A method of performing an operation or a manner of proceeding on a course of action. It differs from policy in that it directs action in a particular situation to perform a specific task within the guidelines of policy. Both policies and procedures are goal-oriented. However, policy establishes limits to action, whereas procedure directs responses within those limits.

## **Profile/Criminal Profile**

An investigative technique used to identify and define the major personality and behavioral characteristics of the criminal offender based on an analysis of the crime(s) he or she has committed.

## **Protocol (of Intelligence Collection)**

Information collection procedures employed to obtain verbal and written information, actions of people, and physical evidence required for strategic and tactical intelligence analysis.

## **Purging (Records)**

The removal and/or destruction of records because they are deemed to be of no further value or because further access to the records would serve no legitimate government interest.

## **Qualitative (Methods)**

Research methods that collect and analyze information that is described in narrative or rhetorical form, with conclusions drawn based on the cumulative interpreted meaning of that information.

## **Quantitative (Methods)**

Research methods that collect and analyze information that can be counted or placed on a scale of measurement that can be statistically analyzed.

## **Racketeer Influenced and Corrupt Organizations (RICO) Act or Similar State Statutes**

Title IX of the Organized Crime Control Act of 1970 (18 U.S.C. Sections 1961-1968) provides civil and criminal penalties for persons who engage in a pattern of racketeering activity or collection of an unlawful debt that has a specified relationship to an enterprise that affects interstate commerce.

## **Racketeering Activity**

State felonies involving murder, robbery, extortion, and several other serious offenses and more than 30 serious federal offenses, including extortion, interstate theft offenses, narcotics violations, mail fraud, and securities fraud.

## **Reasonable Suspicion**

When information exists that establishes sufficient facts to give a trained law enforcement or criminal

investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise.

### **Recommendations**

Suggestions for actions to be taken based on the findings of an analysis.

### **Records (Intelligence)**

See Intelligence Records (Files).

### **Records System**

A group of records from which information is retrieved by reference to a name or other personal identifier, such as a social security number.

### **Red Team**

A technique for assessing vulnerability that involves viewing a potential target from the perspective of an attacker to identify its hidden vulnerabilities and to anticipate possible modes of attack.

### **Regional Information Sharing Systems® (RISS)**

RISS is composed of six regional intelligence centers that provide secure communications, information sharing resources, and investigative support to combat multijurisdictional crime and terrorist threats to over 8,000 local, state, tribal, and federal member law enforcement agencies in all 50 states, the District of Columbia, U.S. territories, Australia, Canada, and England.

### **Regional Intelligence Centers**

Multijurisdictional centers cooperatively developed within a logical geographical area that coordinate federal, state, and local law enforcement information with other information sources to track and assess criminal and terrorist threats that are operating in or interacting with the region.

### **Reliability**

Asks the question, "Is the source of the information consistent and dependable?"

### **Reporting**

Depending on the type of intelligence, the process of placing analyzed information into the proper form to ensure the most effective consumption.

### **Requirements (Intelligence)**

The types of intelligence operational law enforcement elements need from the intelligence function within an agency or other intelligence-producing organizations in order for law enforcement officers to maximize protection and preventive efforts as well as identify and arrest persons who are criminally liable.

### **Responsibility**

Responsibility reflects how the authority of a unit or individual is used and determines whether goals have been accomplished and the mission fulfilled in a manner that is consistent with the defined limits of authority.

### **Risk Assessment**

An analysis of a target, illegal commodity, or victim to identify the probability of being attacked or criminally compromised and to analyze vulnerabilities.

### **Risk Management-Based Intelligence**

An approach to intelligence analysis that has as its object the calculation of the risk attributable to a threat source or acts threatened by a threat source; a means of providing strategic intelligence for planning and policymaking, especially regarding vulnerabilities and countermeasures designed to prevent criminal acts; a means of providing tactical or operational intelligence in support of operations against a specific threat source, capability, or modality; can be quantitative if a proper database exists to measure likelihood and impact and calculate risk; can be qualitative and subjective and still deliver a reasonably reliable ranking of risk for resource allocation and other decision making in strategic planning and for operations in tactical situations.

### **Rules**

A specific requirement or prohibition that is stated to prevent deviations from policy or procedure. A violation of a rule typically results in an internal investigation and may result in disciplinary action.

## Sealing (Records)

Records are stored by an agency but cannot be accessed, referenced, or used without a court order or statutory authority based on a showing of evidence that there is a legitimate government interest to review the sealed information.

## Security

A series of procedures and measures that, when combined, provide protection of people from harm, information from improper disclosure or alteration, and assets from theft or damage. (Criminal Justice Commission, 1995.)

## Sensitive But Unclassified (SBU) Information

Information that has not been classified by a federal law enforcement agency that pertains to significant law enforcement cases under investigation and criminal intelligence reports that require dissemination criteria to only those persons necessary to further the investigation or to prevent a crime or terrorist act.

## Sensitive Compartmented Information (SCI)

Classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems.

## Sensitive Compartmented Information Facility (SCIF)

An accredited area, room, group of rooms, buildings, or an installation where SCI may be stored, used, discussed, and/or processed.

## Sensitive Homeland Security Information (SHSI)

Any information created or received by an agency or any local, county, state, or tribal government that the loss, misuse, unauthorized disclosure, modification of, or the unauthorized access to could reasonably be expected to impair significantly the capabilities and/or efforts of agencies and/or local, county, state, and tribal personnel to predict, analyze, investigate, deter, prevent, protect against, mitigate the effects of, or recover from acts of

terrorism. SHSI does not include any information that is:

1. Classified as national security information pursuant to Executive Order 12958, as amended, or any successor order.
2. Designated by Executive Order 12951, any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. § 2011), to require protection against unauthorized disclosure.
3. Protected Critical Infrastructure Information (PCII) as defined in 6 Code of Federal Regulations (CFR) § 29.2.
4. Sensitive Security Information (SSI) as defined in 49 CFR Part 1520.

## Signal Intelligence (SIGINT)

The interception of various radio frequency signals, microwave signals, satellite audio communications, nonimagery infrared and coherent light signals, and transmissions from surreptitiously placed audio microtransmitters in support of the communications intelligence activity.

## Sources

From an intelligence perspective, these are persons (human intelligence, or HUMINT) who collect or possess critical information needed for intelligence analysis.

## Spatial Analysis

The process of using a geographic information system in combination with crime-analysis techniques to assess the geographic context of offenders, crimes, and other law enforcement activity.

## Statistical System

An organized means of collecting, processing, storing, and retrieving aggregate information for purposes of analysis, research, and reference. No individual records are stored in a statistical system.

## Strategic Intelligence

An assessment of targeted crime patterns, crime trends, criminal organizations, and/or unlawful commodity transactions for purposes of planning, decision making, and resource allocation; the focused examination of unique, pervasive, and/or complex crime problems.

## **Substantive Due Process**

Guarantees persons against arbitrary, unreasonable, or capricious laws, and it acts as a limitation against arbitrary governmental actions so that no government agency may exercise powers beyond those authorized by the Constitution.

## **Surveillance**

The observation of activities, behaviors, and associations of a LAWINT target (individual or group) with the intent to gather incriminating information, or “lead” information, that is used for the furtherance of a criminal investigation.

## **Tactical Intelligence**

Evaluated information on which immediate enforcement action can be based; intelligence activity focused specifically on developing an active case.

## **Target**

Any person, organization, group, crime or criminal series, or commodity being subject to investigation and intelligence analysis.

## **Target Profile**

A profile that is person-specific and contains sufficient detail to initiate a target operation or support an ongoing operation against an individual or networked group of individuals.

## **Targeting**

The identification of crimes, crime trends, and crime patterns that have discernable characteristics that make collection and analysis of intelligence information an efficient and effective method for identifying, apprehending, and prosecuting those who are criminally responsible.

## **Tear-Line Report**

A report containing classified intelligence or information that is prepared in such a manner that data relating to intelligence sources and methods are easily removed from the report to protect sources and methods from disclosure. Typically, the information below the “tear line” can be released as Sensitive But Unclassified.

## **Telemetry**

The collection and processing of information derived from noncommunications electromagnetic

radiations emitting from sources such as radio navigation systems (e.g., transponders), radar systems, and information/data signals emitted from monitoring equipment in a vehicle or device.

## **Telephone Record (Toll)/ Communications Analysis**

An assessment of telephone call activity associated with investigatory targets to include telephone numbers called and/or received, the frequency of calls between numbers, the dates of calls, length of calls, and patterns of use.

## **Third Agency Rule**

An agreement wherein a source agency releases information under the condition that the receiving agency does not release the information to any other agency—that is, a third agency.

## **Threat Assessment**

An assessment of a criminal or terrorist presence within a jurisdiction integrated with an assessment of potential targets of that presence and a statement of probability that the criminal or terrorist will commit an unlawful act. The assessment focuses on the criminal’s or terrorist’s opportunity, capability, and willingness to fulfill the threat.

## **Threat Inventory**

An information and intelligence-based survey within the region of a law enforcement agency to identify potential individuals or groups that pose a criminal or terrorist threat without a judgment of the kind of threat they pose. The inventory is simply to determine their presence.

## **Undercover Investigation**

Active infiltration of or an attempt to infiltrate a group believed to be involved in criminal activity and/or the interaction with a LAWINT target with the intent to gather incriminating information or lead information that is used for the furtherance of a criminal investigation.

## **Validity**

Asks the question, “Does the information actually represent what we believe it represents?”

## **Variable**

Any characteristic on which individuals, groups, items, or incidents differ.

## **Vet**

To subject a proposal, work product, or concept to an appraisal by command personnel and/or experts to ascertain the product's accuracy, consistency with philosophy, and/or feasibility before proceeding.

## **Violent Criminal Apprehension Program (VICAP)**

A nationwide data information center operated by the FBI's National Center for the Analysis of Violent Crime, designed to collect, collate, and analyze specific crimes of violence.

## **Vulnerability Assessment**

An assessment of possible criminal or terrorist group targets within a jurisdiction integrated with an assessment of the target's weaknesses, likelihood of being attacked, and ability to withstand an attack.

## **Warning**

To notify in advance of possible harm or victimization as a result of information and intelligence gained concerning the probability of a crime or terrorist attack.

