COUNTER-TERRORISM TRAINING WORKING GROUP

Global Justice Information Sharing Initiative

United States Department of Justice

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

FINDINGS AND RECOMMENDATIONS

September 2004

Prepared by the Criminal Intelligence Training Coordination Strategy Working Group

Presented to the Counter-Terrorism Training Coordination Working Group and Global Intelligence Working Group

MINIMUM CRIMINAL INTELLIGENCE TRAINING STANDARDS
FOR
UNITED STATES LAW ENFORCEMENT AND OTHER CRIMINAL JUSTICE AGENCIES

REPORT
FINDINGS AND RECOMMENDATIONS

SEPTEMBER 2004

Table of Contents

Preface

Introduction

Minimum Intelligence Training Standards
- Summary
- Intelligence Analyst
- Intelligence Manager
- Law Enforcement Executive
- General Law Enforcement Officer (Basic Recruit and In-Service)
- Intelligence Officer/Collector
- Train-the-Trainer

Conclusion

Appendix
- A: *National Criminal Intelligence Sharing Plan*, Assessment Summary, June 2004
- B: GIWG Training Committee Recommendations
- C: Criminal Intelligence Training Coordination Strategy Questionnaire
- D: Questionnaire Results
- E: Glossary

PREFACE

Over the last several years, the value of criminal intelligence has garnered increased attention within the law enforcement community. Criminal intelligence can link critical information, building a foundation for criminal and terrorist investigations. With this increase in recognition, respect, and demand comes an increased need for adequate training of individuals involved in the collection, analysis, evaluation, and dissemination of intelligence information.

Law enforcement agencies around the country acknowledge that a gap exists in the criminal intelligence training arena. According to an assessment developed to gauge the effect of the *National Criminal Intelligence Sharing Plan*, respondents from the law enforcement community cited the lack of sufficient training for personnel as a significant impediment to enhancing their intelligence function. Respondents stressed the need for intelligence training at all levels of law enforcement.[1]

In order to effectively support criminal and terrorist investigations, law enforcement personnel must receive accurate, timely, and relevant intelligence and information. Information sharing among law enforcement and public safety agencies is a fundamental relationship needed to ensure success. Improving and enhancing criminal intelligence training, through core minimum standards, increase the ability of law enforcement personnel to detect, prevent, and solve crimes, while raising the professionalism and magnitude of the field.

"The significant problems we face cannot be solved at the same level of thinking we were at when we created them."[2] The renewed interest in and support for the intelligence function are significant steps toward overcoming many of the obstacles that criminal intelligence faces, as well as improving our ability to safeguard our homeland. This report reflects the collaborative observations and recommendations pertaining to core minimum criminal intelligence training standards.

---

[1] *National Criminal Intelligence Sharing Plan*, Assessment Summary, June 2004 (*Appendix A*).
[2] Albert Einstein (1879-1955).

LEFT BLANK ON PURPOSE

INTRODUCTION

After September 11, 2001, local, state, tribal, and federal law enforcement agencies realized that they had become too idle in the collection of critical intelligence that could have helped prevent or mitigate the horrible occurrences of that day. There was a public outcry and political demand to greatly enhance the capabilities of law enforcement to gather, store, analyze, and disseminate criminal intelligence information on a timely basis.

Intelligence suddenly became a viable force in protecting our homeland, in addition to its previous role in crime prevention and law enforcement. Various initiatives urged expansion of criminal intelligence sharing, enhanced use of information processing technologies, and increased intelligence training of law enforcement personnel.

In late 2001, law enforcement officials attending the annual conference of the International Association of Chiefs of Police (IACP) identified the need for a comprehensive assessment to ascertain the inadequacies of the criminal intelligence process. As a result, law enforcement executives and intelligence experts met together at the IACP Criminal Intelligence Sharing Summit held in March 2002 and articulated a proposal for an intelligence sharing plan. Summit participants envisioned local, state, and tribal law enforcement agencies fully participating with federal agencies to coordinate, collect, analyze, and appropriately disseminate criminal intelligence information.

Results of the Summit are documented in the August 2002 report entitled "Recommendations From the IACP Intelligence Summit, Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing at the Local, State and Federal Levels." The criminal intelligence sharing report contained a proposal to create a *National Criminal Intelligence Sharing Plan* ("Plan"). Later in 2002, in response to this proposal,

the U.S. Department of Justice (DOJ), Office of Justice Programs (OJP), Bureau of Justice Assistance (BJA), authorized the formation of DOJ's Global Justice Information Sharing Initiative (Global) Intelligence Working Group (GIWG), one of several issue-focused Working Groups of the Global Advisory Committee.

The GIWG was created to examine national criminal intelligence information sharing needs and offer recommendations concerning policies, privacy issues, training, and system integration practices related to intelligence sharing. The initial meeting of the GIWG occurred in December 2002; representatives included officials from all levels of law enforcement, including practitioners, policymakers, and subject-matter experts.

The GIWG formed several committees, including a Training Committee, which recommended the development of minimum training standards for all affected levels of law enforcement personnel. Specifically, the recommendation included establishment of core training objectives in six areas: Law Enforcement Officer, Law Enforcement Executive, Intelligence Commander/Supervisor, Intelligence Officer/Collector, Intelligence Analyst, and Train-the-Trainer. These recommendations are contained in the Plan, which was endorsed by former U.S. Attorney General John Ashcroft, Federal Bureau of Investigation (FBI) Director Robert Mueller, and former U.S. Department of Homeland Security (DHS) Secretary Tom Ridge in October 2003. A National Kick-Off Event was held in May 2004 to recognize the Plan as the blueprint for intelligence sharing for the law enforcement community. The training objectives included in the Plan (*Appendix B*) are considered the foundation for criminal intelligence training standards.

To build upon the core training objectives outlined in the Plan, OJP established another critical initiative known as the Counter-Terrorism Training Coordination Working Group (CTTWG). Recognizing the need for all law enforcement officers and intelligence analysts at the local, state, tribal, and federal levels to increase their knowledge,

awareness, and understanding of terrorism and the need for the integration of critical intelligence information, the CTTWG focuses on maximizing the use of limited resources by ensuring that counter-terrorism training offered by federal agencies conveys a consistent message, is of sufficient quality, and meets the needs of law enforcement and first-responders.

The CTTWG began its efforts by focusing on training currently offered or being contemplated by DOJ components and other justice-related agencies, identifying duplication or gaps, and recommending the most effective mechanism for training delivery.

Since its inception, the CTTWG has expanded its membership and integrated the needs of local and state agencies. It has initiated several projects to further its mission. The CTTWG has searched the Internet, surveyed criminal justice entities, opened communication with constituent agencies, and created a resource Web site.

In November 2003, members of the CTTWG met and surveyed the various types of intelligence-related training courses available through their agencies, courses needed and/or requested by law enforcement personnel, and the need for consistent training standards. During the meeting, the CTTWG authorized the formation of a subgroup—the Criminal Intelligence Training Coordination Strategy (CITCS) Working Group—to focus on developing an intelligence training coordination strategy.

The CITCS met in Arlington, Virginia, on January 8, 2004, to explore criminal intelligence training issues and to begin the development of strategy to coordinate training efforts in furtherance of recommendations outlined in the Plan. Participants were provided an overview of the Plan, with specific emphasis on the core training objectives. CITCS participants shared information regarding criminal intelligence training currently offered or under development by their respective agencies. During the meeting, it became

clear that there were voids in existing criminal intelligence training and duplication of effort in terms of training development and delivery.

To address these issues, CITCS members participated in subcommittees to further identify specific criminal intelligence training needs, including critical issues for consideration. The CITCS recommended that a questionnaire be developed and disseminated to gauge training needs. In addition, the CITCS recommended that the chairman of the GIWG Training Committee be appointed to the CTTWG, to provide a link between the two initiatives and eliminate possible duplication. Further, the CITCS agreed that additional representatives from all levels of law enforcement should be invited to participate in the group's activities.

The CITCS formed four subcommittees to focus on five training classifications: Intelligence Analyst, Intelligence Manager, Law Enforcement Executive, General Law Enforcement Officer (Basic Recruit and In-Service), and Train-the-Trainer. This action was authorized by the CTTWG at its meeting on January 30, 2004.

With the above recommendations approved and instituted, the CITCS met on February 25, 2004, and began broadening the scope of the training objectives. Subcommittees discussed training length, location, and delivery.

The CITCS developed and distributed an automated questionnaire in May 2004 to 200 local, state, and federal law enforcement agencies, as well as training and intelligence organizations (*Appendix C*). The questionnaire focused on the types of training offered or being developed, impediments to training, types of courses offered, and the importance of training at all levels of law enforcement. The results of the CITCS questionnaire (*Appendix D*) confirmed that intelligence training is a critical element in ensuring that the members of the law enforcement community have the appropriate resources and knowledge needed to successfully fulfill their roles and responsibilities.

On June 9, 2004, CITCS participants received the results of the questionnaire. In addition, the four subcommittees convened and finalized their recommendations regarding core minimum training standards. Through the dedication of the participants and supporters of all entities involved, a set of core elements has been vetted and is provided in this report for consideration and endorsement.

One universal issue addressed in each of the subcommittees was the need for a common language. A glossary was created to assist participants and ensure consistent interpretations of intelligence-related terms (*Appendix E*).

The efforts of the CITCS, with the support of the CTTWG and GIWG, are significant steps, not only in implementing the tenets of the Plan but also in building awareness, institutionalizing the importance of criminal intelligence, increasing the value of intelligence personnel, fostering relationships among the law enforcement community, improving the ability to detect and prevent acts of terrorism and other crimes, and creating a safer home for our citizens. The recommendations contained in this document will be forwarded to members of the CTTWG and GIWG for further vetting and endorsement. Upon approval, this document will be made available to the law enforcement community through a variety of outreach efforts.

LEFT BLANK ON PURPOSE

CORE MINIMUM CRIMINAL INTELLIGENCE TRAINING STANDARDS

Described in this portion of the report are recommendations for core minimum criminal intelligence training standards for each training classification:

- Intelligence Analyst
- Intelligence Manager
- Law Enforcement Executive
- General Law Enforcement Officer (Basic Recruit and In-Service)
- Intelligence Officer/Collector
- Train-the-Trainer

The recommendations include objectives, standards, and time allotments for each element, as well as suggested curriculum, training delivery, and materials. Standards are defined as the specific courses or topics of instruction required to meet the training objectives.

The CITCS subcommittees developed standards based on the training objectives outlined in the Plan. These groups considered all facets of the training classifications and discussed specific types of courses and topics needed to provide personnel the basic elements of intelligence.

The purpose of these standards is to provide a blueprint for training facilities, law enforcement agencies, and personnel. These are not mandated standards, but rather, a guide for agencies and organizations to develop and/or enhance their intelligence function. It is important to stress that these are minimum standards. Agencies and organizations may offer course work that exceeds the recommended elements provided herein. Although specialized or advanced training will strengthen personnel and their abilities, the goal of the CITCS is to develop minimum training standards with the intent of creating consistency throughout the criminal intelligence training arena.

LEFT BLANK ON PURPOSE

INTELLIGENCE ANALYST

SUMMARY

Total Course Time Allotment: 40 hours minimum

Time Allotment per Objective:

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

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

4–6 hours **Objective III:** *Analysts will experience the development of intelligence through the processes of critical thinking, logic, inference development, and recommendation development.*

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

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

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

16−18 hours **Objective VII:** *Analysts will demonstrate a practical knowledge of the methods, tools, and techniques employed in analysis, including but not limited to crime pattern analysis, association analysis, telephone record analysis, flow analysis, spatial analysis, financial analysis, and strategic analysis.*

4–8 hours **Objective VIII:** *Analysts will be familiar with the skills underlying analytic methods, including report writing, statistics, and graphic techniques.*

INTELLIGENCE ANALYST

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

Time Allotment for Objective: 3 hours

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Introduction to intelligence	30 minutes	
2. Intelligence process/cycle	60 minutes	• Collection, analysis, dissemination/production, collation/evaluation, assessment • Origin/history of intelligence • Roles and responsibilities of the analyst • Intelligence-led policing
3. Networking	30 minutes	Liaison with peers, other agencies, organizations, and professional memberships for dissemination of information
4. Importance of the *National Criminal Intelligence Sharing Plan* (NCISP)	30 minutes	• Information sharing/information sharing initiatives (LEIS, Global, N-DEx) • Threats facing community, state, nation • Terrorism/topical materials • Intelligence-led policing • Community-oriented policing
5. Professional standards/ certification program for analysts	30 minutes	IALEIA is developing standards to support this requirement

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

Time Allotment for Objective: 1 hour

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Security	30 minutes	
2. Information management	15 minutes	• Electronic • Archives (storage) • Files (hard copy)
3. Evaluation	15 minutes	Reliability/source validity

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

Time Allotment for Objective: 4−6 hours

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Critical thinking	60 minutes	
2. Logic/fallacies of logic	60 minutes	
3. Inference development	60 minutes	
4. Crime indicators	60 minutes	
5. Crime patterns/analysis	60 minutes	

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

Time Allotment for Objective: 1 hour

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Effective planning of intelligence products	30 minutes	Development of collection and investigative plans
2. Needs of the consumer	15 minutes	Does the intelligence product meet the needs of its intended purpose?
3. Infusing consumer feedback into the intelligence cycle	15 minutes	

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

Time Allotment for Objective: 4 hours

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Laws and legal aspects	90 minutes	• Adhering to policies/procedures • 28 CFR Part 23 • Possible resources include U.S. Attorneys' Offices, District Attorneys' Offices, and local prosecutors
2. Courtroom testimony	30 minutes	• Include short role-playing session (Note: if role-playing is used, may need additional time) • Provide "dos" and "don'ts"
3. Ethics	30 minutes	Provide scenario to illustrate importance
4. Privacy issues	30 minutes	Include privacy issues/examples
5. Criminal justice overview	30 minutes	
6. Evidence handling	30 minutes	

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

Time Allotment for Objective: 2 hours

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Sources of information/ available resources	60 minutes	• Internet – search engines, sites • Information sharing systems (RISS, HIDTA, LEO, ATAC, JTTF) • Networks • Centers • Commercial and public databases • Other sources
2. Research methods	30 minutes	• Law enforcement statistics • Managing information
3. New technologies	30 minutes	

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

Time Allotment for Objective: 16–18 hours

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Analytical Techniques	14 hours	• Threat assessments • Crime pattern analysis • Association analysis • Telephone record analysis • Flowchart analysis (event/commodity) • Spatial analysis • Financial analysis • Strategic analysis
2. Analytical tools	2 hours	• Excel/PowerPoint • Flowcharting applications • Analyst notebook, etc.

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

Time Allotment for Objective: 4–8 hours

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Report writing	3 hours	• Principles of good report writing • Differences between intelligence/ investigative reports, briefs, etc.
2. Presentation of information	3 hours	Oral, written, graphics

LEFT BLANK ON PURPOSE

INTELLIGENCE MANAGER

SUMMARY

Total Course Time Allotment: 21 hours with a 3-hour roundtable = 24 hours

The subcommittee recognizes that in most cases, law enforcement agencies will not have a large intelligence function that requires a designated supervisor or manager. For those organizations maintaining large intelligence functions, it is recommended that managers have, at a minimum, the items listed in this section. However, in most cases, agencies have small intelligence functions or no intelligence function. Often, one individual, the Officer-In-Charge (OIC), has the sole responsibility for the intelligence function. In these cases, individuals may not need a 24-hour, classroom-style course. Training for the OIC may be conducted through CD-ROM and other delivery mechanisms.

Time Allotment per Objective:

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

1 hour — **Objective II:** *Managers will be provided with information on training, evaluating, and assessing an effective criminal intelligence function.*

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

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

4 hours — **Objective V:** *Managers will understand the legal and privacy issues surrounding the criminal intelligence environment.*

4 hours — **Objective VI:** *Managers will understand the processes necessary to produce tactical and strategic intelligence products.*

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

3 hours — **Objective VIII:** *Managers will understand the development process and implementation of collection plans.*

INTELLIGENCE MANAGER

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

This objective is an overview of intelligence and sets the stage for the rest of the course.

Time Allotment for Objective: 2 hours

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Definition of intelligence	30 minutes	• Examples of what it is/what it is not • Do not rely on one definition
2. General intelligence process/ cycle	60 minutes	Include impediments to the intelligence process/cycle
3. Why intelligence is important to managers, analysts, executives	15 minutes	Focus on why intelligence is important for the agency and community you serve
4. Intelligence-led policing	15 minutes	• Brief overview/definitions of intelligence-led policing • Community-oriented policing

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

Time Allotment for Objective: 1 hour

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Evaluating intelligence unit performance	30 minutes	Provide handout/checklist; include information regarding performance metrics
2. Personnel training	30 minutes	Informative component; include what executives, analysts, and officers should be trained on and where training is available

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

Time Allotment for Objective: 4 hours

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Intelligence purpose/mission	60 minutes	• Where does intelligence fit in your agency? • Roles/responsibilities of intelligence function • Provide examples of intelligence

		function missions • Write a mission for your intelligence function
2. Building the capacity to achieve the mission	2 hours	• A "Day in the Life of Intel" • Organizational structure • Staffing levels/attributes • Managing resources/task management • Pitfalls/obstacles • Provide example models
3. Operating policies and procedures – mechanics of an intelligence function	60 minutes	• Physical security • File management • Informants • Ethics • Handouts/CDs (i.e., glossary)

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

Time Allotment for Objective: 1 hour

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Handling and storing of information (security, e-mail)	15 minutes	Internet, networks/systems, firewalls
2. Classifications	15 minutes	Secret, Top Secret, National Security Issues (pamphlets from FBI), etc.
3. Operational security processes	30 minutes	• Protecting methods and sources • Policies/rules (i.e., dissemination) • Disclosure of sensitive information to media, other law enforcement entities, citizens, public safety agencies, etc.

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

Time Allotment for Objective: 4 hours—"history lesson" of intelligence

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Legal and historical perceptive	60 minutes	• Answer the "why?" • Provide a story/scenario to illustrate importance of legal/privacy issues • Include issues/examples regarding privacy • Possible resources include U.S. Attorneys' Offices, District Attorneys' Offices, and local prosecutors
2. Current regulations	60 minutes	• Answer the "what?" • Regulations/resources on CD (28 CFR Part 23)

3. Application	60 minutes	• Question and answer • How to put this information into practice
4. Ensuring accountability	60 minutes	Provide checklist to gauge compliance (LEIU is developing the checklist)

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

Time Allotment for Objective: 4 hours

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Types of intelligence products	60 minutes	
2. Principles of good report writing	60 minutes	Provide differences between intelligence/investigative projects/reports, briefs, etc.
3. Uses of intelligence products	60 minutes	Strategic, tactical, operational, data visualization, and value of products
4. Feedback	60 minutes	Does the intelligence product meet the needs of its intended purpose?

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

Time Allotment for Objective: 2 hours

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Sources of information	30 minutes	• Provide overview, resource CD • Include public, commercial, and criminal sources of information
2. Information on existing criminal information sharing initiatives, systems, networks, and resources available	60 minutes	• Overview of NCISP • RISS, HIDTA, LEO, ATAC, JTTF, EPIC, FinCEN, LEIU, IALEIA, INTERPOL, LEIS, N-DEx
3. Networking/relationship building	30 minutes	• Discuss how intelligence is not only technical, it is a human effort • Provide information on associations/ networking opportunities

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

This objective pertains to Requirements Management—pulls all requirements together and explains how to run the intelligence function.

Time Allotment for Objective: 3 hours

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Defining the customers	30 minutes	Understand the needs of the customer and what is important to the customer
2. Methods of collection	60 minutes	Identifying gaps
3. Competing hypothesis	60 minutes	Reliability/validity – ensure analysis is reliable; do not follow a blind alley
4. Threat Assessments	30 minutes	

LEFT BLANK ON PURPOSE

LAW ENFORCEMENT EXECUTIVE

SUMMARY

Total Course Time Allotment: 4 hours

Time Allotment per Objective:

30 min. **Objective I:** *Executives will understand the* National Criminal Intelligence Sharing Plan *(NCISP) and their own role in the NCISP.*

30 min. **Objective II:** *Executives will understand the philosophy of intelligence-led policing.*

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

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

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

30 min. **Question-and-Answer Session**

Recommendations: Instruction block should be referred to as a briefing to include facilitated discussion. If time allows, representatives from local, state, or regional intelligence centers should be invited to make a brief presentation. At a minimum, informational materials should be available for participants. Some of the materials recommended include model policies, guidelines, and glossaries. It is also recommended that a resource guide be provided to attendees that contains items such as the NCISP, COMPSTAT resources, legal/liability resources, 28 CFR Part 23 guidelines, list of networks (why each is important and how they are beneficial), and standards.

Venues for executive education might include U.S. Attorney's Law Enforcement Coordinating Committee (LECC) annual and local meetings; criminal justice academies; Executive Office for United States Attorneys (EOUSA), POST executive education, FBI National Academy and Executive Institute, Law Enforcement Executive Development Seminar (LEEDS) program, COPS Annual Conference and Regional Community Policing Institutes (RCPI), State Chiefs of Police Association meetings, IACP, National Sheriffs' Association (NSA), and other law enforcement organizations' meetings.

Executive curriculum has been developed and a pilot course is scheduled for fall 2004.

LAW ENFORCEMENT EXECUTIVE

Objective I: *Executives will understand the* National Criminal Intelligence Sharing Plan *(NCISP) and their own role in the NCISP.*

Time Allotment for Objective: 30 minutes

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Overview of the NCISP	20 minutes	
2. Impediments to information sharing	10 minutes	• Community-oriented policing

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

Time Allotment for Objective: 30 minutes

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Overview of the philosophy of intelligence-led policing	10 minutes	• The intelligence function • Using intelligence to support and develop policy • Executive leadership roles and responsibilities
2. Overview of information sharing initiatives	10 minutes	Examples – Global, LEIS, N-DEx
3. Overview of best practices in intelligence-led policing	10 minutes	• Discuss initiatives such as COMPSTAT • Community-oriented policing

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

Time Allotment for Objective: 1 hour

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Why intelligence is important to the law enforcement executive	15 minutes	• Types of intelligence (strategic/tactical) • Available products (briefs/reports/charts)
2. Intelligence process/cycle	15 minutes	Evaluating progress/performance
3. Policies and procedures	30 minutes	• Overview of the need for policies and procedures for intelligence officers and intelligence units • Provide glossary/common language as a handout
The following are recommended to be included in the curriculum, but not as specific standards: • Impediments to the intelligence process/cycle • Building a successful intelligence unit • Managing/maximizing intelligence resources		

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

Time Allotment for Objective: 1 hour

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Overview of legal and liability issues, intelligence audits/integrity, accountability, 28 CFR Part 23, and standards for protecting information	45 minutes	• Provide model policy/guidelines as a handout • Possible resources include U.S. Attorneys' Offices, District Attorneys' Offices, and local prosecutors
2. Overview of community trust and communication with citizens and media (briefing city and community leaders on local ordinances)	15 minutes	• Ethics • Public relations (handling difficult situations)

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

Time Allotment for Objective: 30 minutes

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Availability and value of intelligence sharing networks/systems and available resources	10 minutes	• LEIS, LEIU, N-DEx • RISS, JRIES, MATRIX
2. Overview of support materials	10 minutes	Resource guide, contacts, standards, etc.
3. Strategies to build relationships/networking	10 minutes	• Discuss how intelligence is not only technical, it is a human effort • Provide information on associations/networking opportunities

LEFT BLANK ON PURPOSE

GENERAL LAW ENFORCEMENT OFFICER—BASIC RECRUIT

SUMMARY

Total Course Time Allotment: 2 hours

Time Allotment per Objective:

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

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

40 min. **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.*

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

GENERAL LAW ENFORCEMENT OFFICER—BASIC RECRUIT

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

Time Allotment for Objective: 40 minutes

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Officers' roles and responsibilities in the intelligence process/cycle	10 minutes	• Ensure that officers understand the steps of the intelligence cycle • Discuss impediments to the process • Provide a copy of the agency intelligence policy or model intelligence policy • Provide a glossary of intelligence terms
2. Types of intelligence (strategic, tactical)	5 minutes	• Define strategic intelligence • Define tactical intelligence • Provide examples of products
3. Origins/history of intelligence	5 minutes	Overview of the NCISP
4. Importance of intelligence for the law enforcement officer	10 minutes	Provide case examples of why intelligence is important for the agency and community served
5. Community policing and its relationship to the intelligence function	10 minutes	• Maintaining community relations • Define community-led policing • Relationship between intelligence-led policing and community-oriented policing • Case examples

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

Time Allotment for Objective: 10 minutes

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Provide overview of the types of systems available	10 minutes	• Explain the significance of different programs • Types of systems (pointer systems, intelligence systems, etc.) • Discuss systems unique to participants • Provide list or summary of available resources and systems

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.*

Time Allotment for Objective: 40 minutes

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Importance of recording and submitting intelligence information	15 minutes	• Provide a copy of agency communication processes/procedures • Case examples
2. Information collection methods, reporting procedures, use of law enforcement sharing systems (RISS, HIDTA, LEO, ATAC, JTTF)	10 minutes	• Provide techniques to recognize key intelligence and criminal activity • Include use of field interview cards • Provide examples of the intelligence process and how it can be a success
3. Identifying sources of information	10 minutes	• Case examples, videos • Provide instruction for understanding current threats • Provide information on local/state/ regional/federal systems and networks • Online resources • Public/commercial data
4. Understanding terminology	5 minutes	• Define intelligence—what is and what is not intelligence—provide examples of products • Define intelligence-led policing • Develop glossary in form of pocket guide

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

The subcommittee recommends legal council/advisor instruction for this Objective. Additional resources may include U.S. Attorneys' Offices, District Attorneys' Offices, and local prosecutors.

Time Allotment for Objective: 30 minutes

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Ethics	5 minutes	Explain why ethics is pertinent to information handling
2. Legal basis, limitations, and liability issues	10 minutes	• Use legal advisor, if available • Include current regulations and provide copies of key regulations, as appropriate
3. 28 CFR Part 23	5 minutes	• General overview of 28 CFR Part 23 • Provide copy of regulation
4. Right to privacy and protection of personal liberties – current privacy initiatives/concerns	10 minutes	• Include issues/examples regarding privacy • Video—immigrant interview contrasting rights in the United States and their country of origin, particularly the First and Fourth Amendment rights

LEFT BLANK ON PURPOSE

GENERAL LAW ENFORCEMENT—
IN-SERVICE

SUMMARY

Total Course Time Allotment: 2 hours

The subcommittee felt that veteran officers not receiving recruit academy training conforming to the basic core training standards should receive training within the agency's annual in-service training cycle. All other officers should receive updates in all areas of basic instruction, highlighting current threats, indicators, trends, and new technology. This assures that all officers receive a reiteration of basic training and necessary updates on a continuing basis. The recommendations below are for refresher training of previously trained officers. This coursework applies to sergeants, lieutenants, officers, and other sworn personnel as deemed appropriate by the employing agency.

Time Allotment per Objective:

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

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

40 min. **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.*

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

GENERAL LAW ENFORCEMENT—IN-SERVICE

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

Time Allotment for Objective: 40 minutes

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Officers' roles and responsibilities in the intelligence process/cycle	10 minutes	• Ensure that officers understand the steps of the intelligence cycle • Discuss impediments to the process • Provide a copy of the agency intelligence policy or model intelligence policy • Provide a glossary of intelligence terms
2. Types of intelligence (strategic, tactical)	5 minutes	• Define strategic intelligence • Define tactical intelligence • Provide examples of products
3. Origins/history of intelligence	5 minutes	Overview of the NCISP
4. Importance of intelligence for the law enforcement officer	10 minutes	Provide case examples of why intelligence is important for the agency and community served
5. Community policing and the criminal intelligence collection function	10 minutes	• Maintaining community relations • Define community-led policing • Relationship between intelligence-led policing and community-oriented policing • Case examples

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

Time Allotment for Objective: 10 minutes

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Provide overview of the types of systems available	10 minutes	• Explain the significance of different programs • Types of systems (pointer systems, intelligence systems, etc.) • Discuss systems unique to participants • Provide list or summary of available resources and systems

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.*

Time Allotment for Objective: 40 minutes

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Review importance of recording and submitting intelligence information	15 minutes	• Provide a copy of agency communication processes/procedures • Case examples
2. Update on information collection methods, reporting procedures, use of law enforcement sharing systems (RISS, HIDTA, LEO, ATAC, JTTF)	10 minutes	• Provide techniques to recognize key intelligence and criminal activity • Include use of field interview cards • Provide examples of the intelligence process and how it can be a success
3. Review the identification of sources of information	10 minutes	• Case examples, videos • Provide instruction in understanding current threats • Provide information on local/state/regional/ federal systems and networks • Online resources • Public/commercial data
4. Review and update of terminology	5 minutes	• Define intelligence—what is and what is not intelligence—provide examples of products • Define intelligence-led policing • Develop glossary in form of pocket guide

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

The subcommittee recommends legal council/advisor instruction for this Objective. Additional resources may include U.S. Attorneys' Offices, District Attorneys' Offices, and local prosecutors.

Time Allotment for Objective: 30 minutes

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Ethics	5 minutes	Explain why ethics is pertinent to information handling
2. Update on legal basis, limitations, and liability issues	10 minutes	• Use legal advisor, if available • Include current regulations and provide copies of key regulation, as appropriate
3. Update 28 CFR Part 23	5 minutes	• General overview of 28 CFR Part 23 • Provide copy of regulation
4. Review right to privacy and protection of personal liberties—current privacy initiatives/concerns	10 minutes	• Include issues/examples regarding privacy • Video—immigrant interview contrasting rights in the United States and their country of origin, particularly the First and Fourth Amendment rights

LEFT BLANK ON PURPOSE

INTELLIGENCE OFFICER/COLLECTOR

SUMMARY

Total Course Time Allotment: 40 hours minimum

Time Allotment per Objective:

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

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

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

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

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

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

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

A 3-hour roundtable discussion is recommended.

NOTE: The CITCS was not tasked with developing standards for the Intelligence Officer/Collector classification. However, the *National Criminal Intelligence Sharing Plan* includes this training classification. The GIWG Training and Outreach Committee reviewed the training objectives for this classification and provided standards for each objective. The standards are consistent with similar objectives contained under the five other training classifications. For ease of use, the standards for the Intelligence Officer/Collector have been included in this report.

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

Time Allotment for Objective: 5 hours

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Introduction to intelligence	60 minutes	• Origin/history of intelligence • Provide a glossary of intelligence terms
2. Intelligence officers' roles and responsibilities in the intelligence process/cycle	60 minutes	• Ensure that intelligence officers understand the steps of the intelligence cycle • Discuss impediments to the process • Provide a copy of the agency intelligence policy or model intelligence policy
3. Importance of intelligence for the intelligence officer	60 minutes	• Provide case examples of why intelligence is important for the agency and community served
4. Community policing and its relationship to the intelligence function	60 minutes	• Maintaining community relations • Define community-led policing • Relationship between intelligence-led policing and community-oriented policing • Case examples
5. Networking	60 minutes	• Liaison with peers, other agencies, organizations, and professional memberships for dissemination of information • Allow participants to discuss the ways their agency networks

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

Time Allotment for Objective: 6 hours

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Ethics	60 minutes	Explain why ethics is pertinent to information handling
2. Legal basis, limitations, and liability issues	60 minutes	• Use legal advisor, if available • Include current regulations and provide copies of key regulations, as appropriate • Possible resources include U.S. Attorneys' Offices, District Attorneys' Offices, and local prosecutors
3. Adhering to policies/ procedures	60 minutes	Provide model policies

4. 28 CFR Part 23	60 minutes	• General overview of 28 CFR Part 23 • Provide copy of regulation
5. Right to privacy and protection of personal liberties – current privacy initiatives/concerns	60 minutes	• Include issues/examples regarding privacy • Video—immigrant interview contrasting rights in the United States and their country of origin, particularly the First and Fourth Amendment rights
6. Courtroom testimony	60 minutes	• Include short role-playing session • Provide "dos" and "don'ts"

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

Time Allotment for Objective: 4 hours

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Sources of information/ available resources	90 minutes	• Internet – search engines, sites • Information sharing systems (RISS, HIDTA, LEO, ATAC, JTTF) • Networks • Centers • Commercial and public databases • Other sources
2. Overview of the NCISP	60 minutes	
3. Research methods	90 minutes	• Law enforcement statistics • Managing information

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

Time Allotment for Objective: 6 hours

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Handling evidence/intelligence	2 hours	
2. Security	60 minutes	
3. Information management	2 hours	• Electronic • Archives (storage) • Files (hard copy)
4. Evaluation	60 minutes	Reliability/source validity

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

Time Allotment for Objective: 6 hours

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Types of intelligence products	60 minutes	
2. Principles of good report writing	2 hours	Provide differences between intelligence/investigative projects/ reports, briefs, etc.
3. Uses of intelligence products	2 hours	• Strategic, tactical, operational, data visualization, and value of products • Threat assessments
4. Feedback	60 minutes	Does the intelligence product meet the needs of its intended purpose?

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

Time Allotment for Objective: 5 hours

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Critical thinking	60 minutes	
2. Logic/fallacies of logic	60 minutes	Analysis of competing hypotheses
3. Inference development	60 minutes	
4. Recommendations development	60 minutes	
5. Crime indicators	60 minutes	

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

Time Allotment for Objective: 5 hours

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Developing collection and investigative plans	4 hours	Class exercise – develop a collection plan
2. Needs of the consumer	30 minutes	Does the intelligence product meet the needs of its intended purpose?
3. Infusing consumer feedback into the intelligence cycle	30 minutes	

TRAIN-THE-TRAINER

SUMMARY

Total Course Time Allotment: 2 days (16 hours)

The subcommittee agreed that the 40 hours of training suggested in the NCISP was too lengthy. They recommend a 2-day, 16-hour course for the Train-the-Trainer objectives. It was agreed that the Train-the-Trainer program should be for locally certified or otherwise qualified instructors. Instructors are expected to be professional and knowledgeable in the field of intelligence and possess both practical and theoretical expertise.

Time Allotment per Objective:

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

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

5 hours — **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.*

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

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

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

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

1 hour — **Objective IX:** *Trainers will prepare and present a short module on intelligence.*

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

Time Allotment for Objective: 2 hours

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Intelligence process/cycle	60 minutes	• Ensure trainers fully understand and can apply the steps of the intelligence cycle • Include the roles and responsibilities of intelligence personnel • Impediments to the process • Case examples; videos
2. Origin/history of intelligence	30 minutes	
3. Why intelligence is important	30 minutes	• Provide examples of why intelligence is important to different people/groups—executives, policymakers, investigators, analysts, etc. • Case examples

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

Time Allotment for Objective: 1 hour

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Overview of the *National Criminal Intelligence Sharing Plan* and information sharing initiatives and systems	30 minutes	• Distribute the NCISP • Include information regarding other information sharing initiatives and systems, such as LEIS, Global, and N-DEx
2. Intelligence-led policing, community policing, and their relationship to intelligence	30 minutes	• Define intelligence-led policing • Discuss benefits of intelligence-led policing

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.*

Time Allotment for Objective: 5 hours

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Intelligence sharing systems	60 minutes	• RISS, HIDTA, LEO, ATAC, JTTF • How to access and use information retrieved from available systems

2. Sources of information	60 minutes	• Internet/networks • Centers • Commercial and public databases • Other sources
3. Current threats, trends, and patterns	60 minutes	
4. Internet navigation and use	60 minutes	
5. New technologies	60 minutes	

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

Time Allotment for Objective: 2 hours

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Analytical tools and techniques, such as flowcharts (event, association, commodity)	60 minutes	• Developing/using flowcharts • Discuss example scenarios—instructor-led application/resolution of exercises
2. Intelligence products (intelligence reports, data/link analysis, etc.)	60 minutes	Developing intelligence reports, differences between intelligence reports, briefs, etc.

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

Time Allotment for Objective: 3 hours

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Current innovations and instructional techniques	60 minutes	ODP training catalog
2. Audiovisual aids, instructional media, and their use	2 hours	• Familiarity with a variety of audiovisual aids • Troubleshooting technical issues • Training materials package

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

Time Allotment for Objective: 1 hour

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Familiarity with existing curricula, lesson plans, tests, and exercises	60 minutes	• Handouts with lesson plans, materials, and exercise demonstrations • Understand what types of training are offered and by whom

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

The subcommittee recommends legal council/advisor instruction for those aspects related to state or federal law. Additional resources may include U.S. Attorneys' Offices, District Attorneys' Offices, and local prosecutors.

Time Allotment for Objective: 1 hour

Standards	Time Allocation	Suggested Curriculum/Sources of Information
1. Legal basis and limitations	10 minutes	• Current regulations and how they apply to intelligence • Intelligence audits/integrity
2. Liability issues	10 minutes	Standards for protecting information
3. 28 CFR Part 23	10 minutes	Provide copy of guideline
4. Right to privacy and protection of personal liberties (examples of privacy issues/initiatives)	20 minutes	• Provide scenarios illustrating privacy issues • Discuss strategy to protect personal information
5. Ethics	10 minutes	

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

Time allotment for Objective: 1 hour

Trainers will provide participants with topics or allow students to choose topics for presentation. Participants may use multimedia. The length of presentations is dependent upon the number of participants and remaining time available.

CONCLUSION

As the area of intelligence continues to develop and grow, intelligence personnel will continue to require consistent, high-quality, and comprehensive instruction. The standards recommended in this report are the first steps in creating a foundation for criminal intelligence training.

The CITCS, a diverse group of local, state, tribal, and federal law enforcement practitioners, experts, and constituent groups, reviewed the standards contained in this report. The standards represent the basic elements required for each training classification (Intelligence Analyst, Intelligence Manager, Law Enforcement Executive, General Law Enforcement Officer, and Train-the-Trainer).

Managers and executives can utilize these standards as a blueprint in determining the types of training needed for their personnel. In addition, training facilities may want to utilize these standards when developing new courses. Individuals entering or wishing to enter the criminal intelligence field may consider using these minimum standards as a baseline for determining the training and education they will need. Again, these standards are not mandatory; they are designed to be a guide for the law enforcement community.

Once these core minimum standards are endorsed by the CTTWG and GIWG, these standards will be shared globally with the law enforcement community. Additional steps in this process may include the development of training curricula, a nationwide training delivery plan, and development of online or Web-based instruction.

It is clear that the collection, evaluation, analysis, and dissemination of intelligence information are critical to our nation's law enforcement efforts and anti-terrorism initiatives. The goal of this initiative is to support these efforts and provide guidance and appropriate training to our law enforcement and intelligence communities.

APPENDIX A

National Criminal Intelligence Sharing Plan, Assessment Summary, June 2004

Global Justice Information Sharing Initiative Intelligence Working Group

National Criminal Intelligence Sharing Plan

Assessment Summary
June 2004

During the tragic events of September 11, 2001, it became painfully clear that sharing information and intelligence is a vital element in detecting, preventing, and apprehending terrorists and other criminals. In spring 2002, the International Association of Chiefs of Police (IACP) met and agreed that a concerted effort must be made to create a collective and collaborative information sharing plan. In response, the Global Justice Information Sharing Initiative (Global) Intelligence Working Group (GIWG) was formed. Through the GIWG's efforts, the *National Criminal Intelligence Sharing Plan* (NCISP or "Plan") was developed, and in October 2003, Attorney General John Ashcroft approved the Plan.

As part of the GIWG's effort to implement the components of the NCISP, members who attended the December 12, 2003, GIWG Executive Steering Committee meeting requested the Institute of Intergovernmental Research to develop an assessment tool to gauge the progress and impact of the NCISP.

From January to April 2004, an assessment tool was developed and disseminated to 217 agencies, consisting of local, state, and federal law enforcement agencies, as well as police organizations and associations. A total of 74 agencies, or 34 percent, responded. The following summarizes the breakdown of agency types that responded to the assessment:

Agency Type	**# of Responses**
Local	37
State	28
Federal	6
Organizations/Associations	3
TOTAL	74

Assessment responses have been aggregated and will not be attributed to a specific agency. Additionally, individual assessment results will not be made public. The following analysis summarizes the responses, observations, and findings of the NCISP assessment.

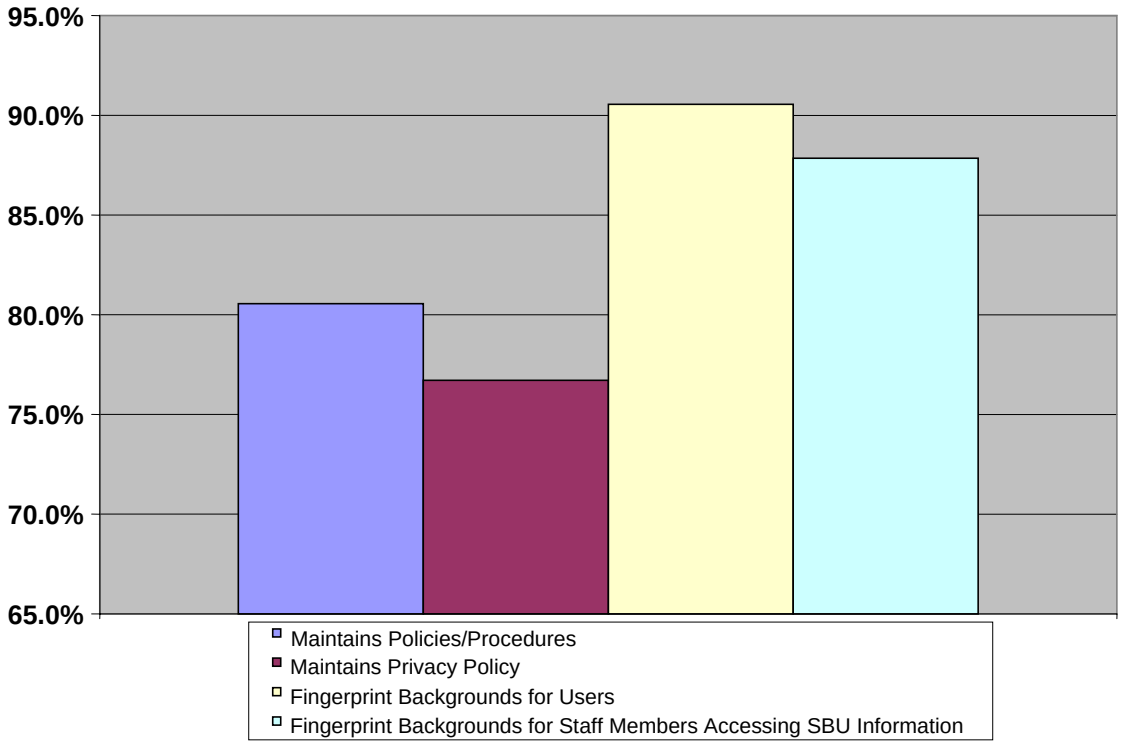
Awareness

The first few questions of the assessment focused on NCISP awareness and progress. Only 67.6 percent of agencies responding indicated that they were familiar with the NCISP. Nineteen of the twenty-two agencies indicating they were not aware of the Plan were local agencies. These results appear to indicate that additional outreach should

be done to target local agencies. Additionally, 58.6 percent of the responding agencies indicated they had implemented portions of the Plan.

Ninety-five percent of the respondents maintain an intelligence function, yet only 56.2 percent stated that their agency had a mission statement addressing intelligence sharing. *Figure 1* indicates that 80.6 percent of the responding agencies maintain policies and procedures, including privacy guidelines, as a framework for their intelligence function. In addition, 90.5 percent of the responding agencies conduct fingerprint background checks on users of information and intelligence systems, while 87.8 percent conduct fingerprint background checks on staff members that have access to sensitive but unclassified (SBU) information sharing capabilities. It appears that the responding agencies support the Plan and are encouraged by its possibilities. A number of the agencies have initiated information sharing programs within their agency or region. The majority appear to recognize the importance of information sharing.

Figure 1



Available Resources

In addition to determining whether agencies were aware of the NCISP, the assessment instrument asked agencies whether they utilized some of the models and guidelines supported by the NCISP. *Figure 2* provides the percentage of agencies that have utilized these models or guidelines.

Figure 2

National Criminal Justice Association (NCJA) - *Justice Information Privacy Guideline – Developing, Drafting and Assessing Privacy Policy for Justice Systems*	19.4%
Federal Regulation 28 Code of Federal Regulations (CFR) Part 23 – Criminal Intelligence Systems	84.5%
Law Enforcement Intelligence Unit (LEIU) standards for intelligence file maintenance	62.5%
Global's *Applying Security Practices to Justice Information Sharing* (Draft)	17.6%
Global Justice Extensible Markup Language (XML) Data Model (Global JXDM)	23.2%
Global Justice XML Data Dictionary (Global JXDD)	20.9%
IACP Criminal Intelligence Model Policy	35.8%

As shown in *Figure 2*, only 19.4 percent of the respondents indicated they had used the National Criminal Justice Association's model privacy policy guidelines. Furthermore, only 17.6 percent stated they had utilized Global's security guidelines. Both privacy and security are critical to successful information sharing. Additional education in these areas, as well as dissemination of these guidelines to a wider audience, may be appropriate.

Less than a quarter (23.2%) of respondents indicated use of the Global Justice Extensible Markup Language (XML) Data Model (Global JXDM). Thirty local agencies, sixteen state agencies, and two federal agencies indicated they were not utilizing the Global JXDM, although some had indicated they were researching the matter. This model may become the primary infrastructure for linking disparate systems. This issue may require additional education to those unfamiliar with the Global Initiative and the Global JXDM.

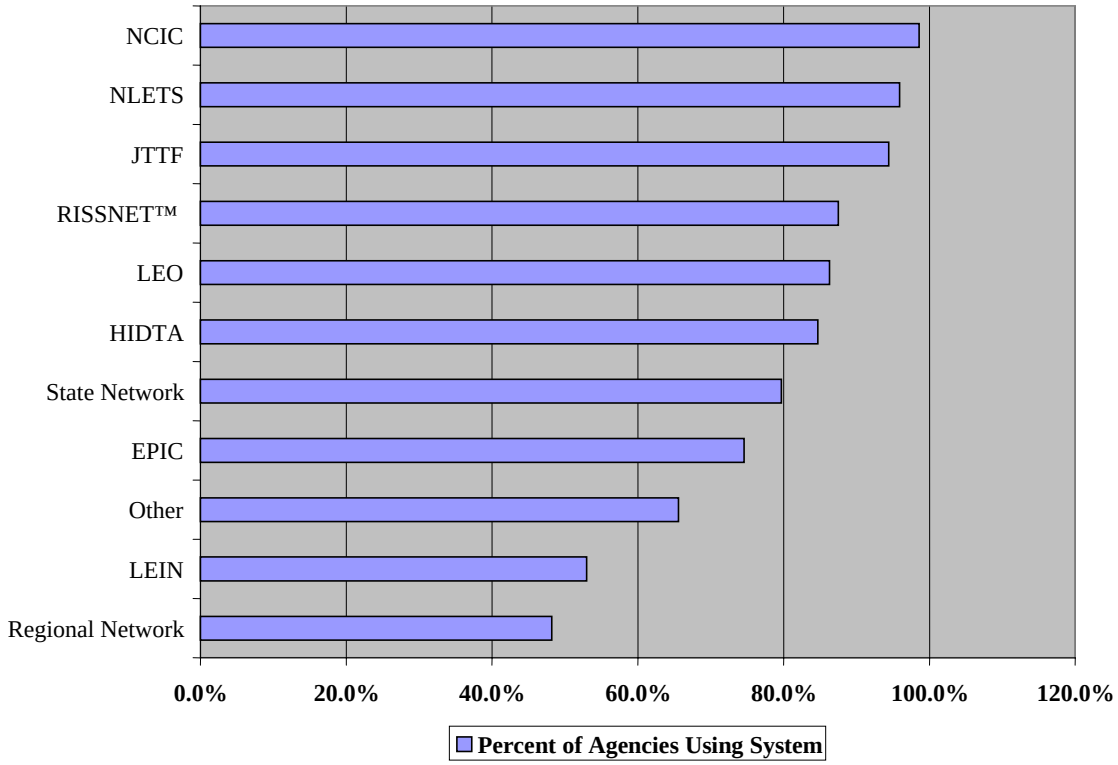
Intelligence Functions

Ninety-five percent of the respondents stated their agency had an intelligence function, but only 80.8 percent indicated their agency currently uses an automated system as part of its intelligence function. One agency indicated a database was under development. Only 76.8 percent of the respondents stated that their agency would be willing to provide access to information and/or intelligence systems through a nationwide information sharing capability. Many agencies stipulated that access and security would be a critical issue prior to allowing access to systems. In addition, legal issues and technical capability were cited as concerns. Other respondents stated that providing access would depend on the extent of the access and how the information would be utilized. Pointer systems were listed as possible solutions. Some agencies indicated the need for a signed memorandum of understanding (MOU) agreement, while others stressed the need to follow 28 CFR Part 23 guidelines, as well as any other appropriate policies.

Intelligence Systems

Figure 3 provides the percentage of responding agencies that utilize specific information and intelligence systems or networks. The chart lists the systems from the least used to the most used.

Figure 3



The percentage of respondents indicating that their agency utilizes the National Criminal Information Center (NCIC) was 98.6 percent, and 95.9 percent utilizes the National Law Enforcement Telecommunication System (NLETS). The Regional Information Sharing Systems network (RISSNET), Law Enforcement Online (LEO), and High Intensity Drug Trafficking Areas (HIDTA) were also rated high. Almost 66 percent indicated their agency utilized other systems not included in the assessment instrument. Some of the systems listed included Financial Crimes Enforcement Network (FinCen), Interpol, Joint Regional Information Exchange System (JRIES), and Multistate Anti-Terrorism Information Exchange (MATRIX).

Information Sharing Improvements

A section of the assessment focused on whether agencies believed certain aspects of information sharing had improved since September 11, 2001. Respondents were asked to indicate whether an impediment had *no change*, was *somewhat better*, or was *significantly better*.

- ✓ 54.2 percent believed that the exchange of information/intelligence between state and local law enforcement agencies was *somewhat better.*
- ✓ 58.3 percent believed that the exchange of information/intelligence between their agency and federal agencies was *somewhat better.*
- ✓ 30.6 percent thought that there was *no change* in technology and equipment availability.
- ✓ 56.9 percent thought that interconnectivity among law enforcement had improved, but 36.1 percent felt there was *no change* in this area.
- ✓ Nearly half (49.3 percent) believed that no change had occurred in the development of standards for intelligence functions.
- ✓ 97.2 percent believed that the working relationships and communications among law enforcement agencies and other local, state, and federal agencies were either *somewhat* or *significantly better.*

Agencies were asked to explain how their organization has improved communication and information sharing. Some have built networks and relationships with other intelligence personnel from regional, state, and federal agencies. Other respondents publish regular intelligence briefs and bulletins and disseminate those to other criminal justice organizations. Many stated that intelligence personnel attend regular regional meetings, participate on multiagency task forces, and are members of professional organizations. Some agencies maintain dedicated intelligence personnel or utilize intelligence liaison officers to bridge communication with field operations. Finally, a number of agencies utilize intelligence databases, a shared network, or an Internet-based application in facilitating their intelligence function.

In general, it appears that the responding agencies have been proactive in developing and fostering partnerships while enhancing their capability of sharing information. Agencies were asked what types of intelligence or information sharing systems or networks they would like to access but do not do so at this time. The responses are summarized in *Figure 4*.

Figure 4

All federal systems (i.e., U.S. Department of Homeland Security, Federal Bureau of Investigation, Social Security, Immigration, U.S. Secret Service, and Customs and Border Patrol)
Employment information and utility databases
Secure Internet Protocol Router Network (SIPERNET), Joint Automated Booking System (JABS), Executive Office for the United States Attorneys (EOUSA)/Electronic Client Management System (ECMS)
Analyst Notebook, Bridge, LexisNexis
MATRIX
Face recognition software
JRIES
Terrorism Screening Center Database

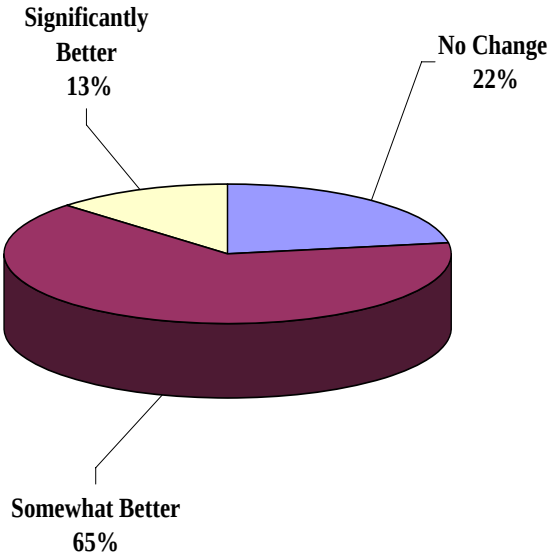
Internal Revenue Service (IRS)
Treasury Enforcement Communications System (TECS)
Narcotics and Dangerous Drugs Information System (NADDIS)
LEIU, RISSNET™, LEO, FinCen
Corrections, parole/probation, and court databases

A number of respondents mentioned that the problem is not that there is insufficient information but that there are too many systems and too many access points. There is confusion about what is needed and what is not needed. Some agencies were not sure what they needed because they did not know enough about available systems.

Intelligence Training Opportunities

As shown in *Figure 5*, almost 65 percent of the responding agencies indicated that intelligence training opportunities were *somewhat better* since September 11. Twenty-two percent, however, indicated *no change*. This was confirmed by the numerous statements from responding agencies regarding a lack of sufficient training for personnel, including executive and legislative levels. Agencies stressed the need for intelligence training at all levels of law enforcement. One agency recommended establishing training at the basic law enforcement academies and focusing particularly on community-oriented policing efforts. Although the overwhelming comments focused on the need for more training, 87.5 percent of the respondents indicated their personnel had received intelligence training within the last year.

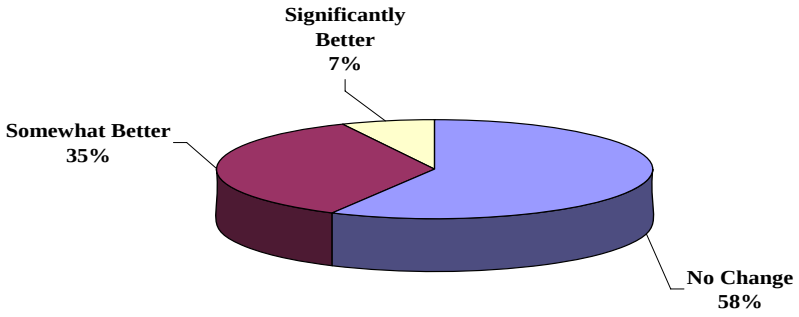
Figure 5



Availability of Personnel

Eighty-six percent of the respondents stated their agency had full-time employees dedicated to the intelligence function. However, as depicted on *Figure 6*, almost 58 percent of the respondents reported there has been *no change* in the availability of intelligence personnel since September 11. The majority of respondents stated that manpower is limited and has resulted in a reactive capability instead of a proactive or prevention effort. Many agencies indicated the need to hire additional analysts and officers but cited lack of funding as an impediment. One agency stated, "Personnel resources are diminishing and the needs for intelligence are growing." Based on these remarks and the need for personnel, it may be worthwhile to develop intelligence function models, providing suggestions on how to create, staff, and manage an intelligence function.

Figure 6



NCISP Improvements

As part of the assessment, agencies were asked to offer suggestions on how to improve the NCISP. Some agencies believed their knowledge of the NCISP was limited and chose not to provide suggestions at this time. A number of agencies, however, provided ideas for consideration.

A couple of agencies stressed the need to ensure proper dissemination of the Plan to all levels of law enforcement. One agency recommended developing best-practices examples to help agencies use common standards. It was also recommended that an accreditation process for intelligence units be adopted, similar to the American Society of Crime Lab Directors (ASCLD) for crime laboratories or the Commission on Accreditation for Law Enforcement Agencies, Inc. (CALEA) for law enforcement agencies.

One area that impacts future planning for the GIWG is the need for implementation plans. Agencies indicated a need for assistance in implementing the Plan and creating intelligence units.

The GIWG was encouraged to continue to be the vocal advocate of the program and to urge all local, state, tribal, and federal law enforcement organizations to participate to the maximum extent possible. Some urged the GIWG, however, not to lock agencies into a single format or philosophy. One agency requested that an overview of the NCISP be presented to their advisory board, and still another offered to assist the GIWG with committee work. Finally, it was recommended that a fusion center be established in each state that would be responsible for centralized processing of information. This fusion point would facilitate bilateral information exchange between the local, state, and federal entities.

Critical Issues

An overwhelming majority of the respondents cited funding as a primary impediment to enhancing their intelligence function. Lack of personnel, limited training, and inadequate equipment and software were also mentioned.

Some agencies explained the need to consolidate or centralize databases and systems. Based on comments from the assessment, there are too many systems; a concerted effort should be made to identify the key systems and consolidate access, creating a "one-stop shopping" capability for agencies. Standardized data exchange models should be developed and deployed to enhance communication and information sharing. Interoperability was mentioned as a critical component for communication and information sharing. Some respondents stressed the need for more sharing of intelligence and increased federal and major city participation.

One area discussed was the concerns regarding the balance of law enforcement access to data sources versus individual rights to privacy. Trust among law enforcement agencies was stressed, as well as the need for a collaborative exchange of information. Many agencies mentioned that in the past, law enforcement agencies were resistant to change and were reluctant to share information. Respondents agreed that law enforcement must build relationships, trust each other, and work together in order to succeed. Some respondents have seen improvements in this area. All the issues raised were valid and insightful and will assist in future planning efforts.

Conclusion

Through this assessment process, it can be concluded that the NCISP is a useful tool for law enforcement. A majority of agencies were familiar with the Plan and support its recommendations. Through continued dissemination of and education about the Plan, more agencies will realize the benefits of adopting the recommendations. However, the impediments identified through the assessment must play a part in implementing the NCISP. Solutions to these issues will need to be addressed in order for the NCISP to become an institution within all levels of law enforcement. The responding agencies recognize the need for this type of partnership and information exchange and appear willing to assist in this effort.

APPENDIX B

For the *GIWG Training Committee Recommendations*, please visit
http://it.ojp.gov/documents/ncisp/criminal_intel_training_standards.pdf

APPENDIX C

Criminal Intelligence Training Coordination Strategy Questionnaire

Criminal Intelligence Training Coordination Strategy Questionnaire

Name of Agency	
Agency Address	
City, State, and Zip	
Name of Person Completing Survey	
Title	
Telephone Number/Extension	
E-Mail Address	

<u>Please complete the following questions</u>.

1. Does your organization deliver criminal intelligence training? ❑ Yes ❑ No ❑ N/A

2. If you answered Yes to Question 1, please indicate which type(s) of intelligence training your organization delivers. Check all that apply.

- ❑ Intelligence Analyst
- ❑ Intelligence Manager
- ❑ Agency Head/Executive
- ❑ General Law Enforcement Recruit
- ❑ General Law Enforcement In-Service
- ❑ Intelligence Train-the-Trainer

3. If you do not deliver training, does your organization plan to develop and deliver criminal intelligence training in the next 12 months? ❑ Yes ❑ No ❑ N/A

4. If you answered Yes to Question 3, please indicate which types(s) of intelligence training your organization plans on delivering. Check all that apply.

- ❑ Intelligence Analyst
- ❑ Intelligence Manager
- ❑ Agency Head/Executive
- ❑ General Law Enforcement Recruit
- ❑ General Law Enforcement In-Service
- ❑ Intelligence Train-the-Trainer

5. Do you believe you have access to appropriate training and training resources to adequately meet your criminal intelligence training needs? ❑ Yes ❑ No ❑ N/A

6. If you answered No to Question 5, please indicate which training types are lacking. Select all that apply. ❑ NA

- ❑ Intelligence Analyst
- ❑ Intelligence Manager
- ❑ Agency Head/Executive
- ❑ General Law Enforcement Recruit
- ❑ General Law Enforcement In-Service
- ❑ Intelligence Train-the-Trainer

7. If you answered No to Question 5, indicate why. Choose all that apply.

- ❑ Difficulty finding good trainers
- ❑ Travel and lodging costs
- ❑ Lack of funding
- ❑ Not sure what types of training are offered
- ❑ Not sure what types of training our personnel should receive
- ❑ Other_____

8. If your agency delivers intelligence training, how often is training offered?

❑ Monthly ❑ Semiannually ❑ Other _____
❑ Quarterly ❑ Annually

9. If your organization delivers intelligence training, select the primary components included in your curriculum. Indicate Not Applicable (N/A) if your organization does not deliver training in that area.

Type	Key Components	
Intelligence Analyst ❑ N/A	❑ Criminal Justice Overview ❑ Introduction to Intelligence ❑ Intelligence Cycle ❑ Intelligence Sharing Systems ❑ Developing Flowcharts ❑ Creating Intelligence Reports	❑ Data Analysis/Link Analysis ❑ Knowledge of Laws and Legal Issues ❑ Report Writing ❑ Oral Presentation Skills ❑ Other _____
Intelligence Manager ❑ N/A	❑ Intelligence Products ❑ Laws, Ethics, and Policy ❑ Handling/Storing Information ❑ Classifications ❑ Intelligence Purpose/Mission ❑ Intelligence Sharing Systems	❑ Common Language ❑ Available Resources ❑ Requirements Management ❑ New Technologies ❑ Security ❑ Other _____
Agency Head/ Executive ❑ N/A	❑ Leadership Role ❑ Intelligence Function and Process ❑ Legal and Liability Issues ❑ Communication to Citizens/Media ❑ Available Resources	❑ Intelligence-Led Policing ❑ Integrity and Accountability ❑ Intelligence Sharing Networks ❑ Other _____
General Law Enforcement Recruit ❑ N/A	❑ Understanding Current Threats ❑ Recording and Disseminating Intelligence ❑ Reporting Procedures ❑ Community-Oriented Policing	❑ Collection Methods ❑ Legal Limitations/Liability ❑ Privacy Issues ❑ Other _____
General Law Enforcement In-Service ❑ N/A	❑ Intelligence Sharing Systems ❑ Intelligence Cycle ❑ Legal Limitations and Liability	❑ Privacy Issues ❑ Maximizing Intelligence Process ❑ Other _____
Intelligence Train-the-Trainer ❑ N/A	❑ Intelligence Sharing Systems ❑ Analytical Techniques/Tools ❑ Topical Materials ❑ Teaching/Adult Education	❑ Legal Basis and Limitations ❑ Liability Issues ❑ Privacy Issues ❑ Other _____

10. Rate the importance of establishing minimum training standards for the following training types. (1 indicates not important; 5 indicates very important)

		Not Important				Very Important
a.	Intelligence Analyst	1	2	3	4	5
b.	Intelligence Manager	1	2	3	4	5
c.	Agency Head/Executive	1	2	3	4	5
d.	General Law Enforcement Recruit	1	2	3	4	5
e.	General Law Enforcement In-Service	1	2	3	4	5
f.	Intelligence Train-the-Trainer	1	2	3	4	5

11. Prioritize the following list of training levels based on your agency's need. Use each number 6 through 1 only once. (6 indicates highest priority; 1 indicates least priority)

___Intelligence Analyst
___Intelligence Manager
___Agency Head/Executive
___General Law Enforcement Recruit
___General Law Enforcement In-Service
___Intelligence Train-the-Trainer

12. What method of delivery do you prefer? Check all that apply.

- ❑ Hands-on, instructor-led in classroom
- ❑ Computer-based
- ❑ Web-based/Online
- ❑ Bulletin boards or mailing lists
- ❑ Workbooks or other training publications
- ❑ Video teleconferencing
- ❑ CD
- ❑ Video/DVD
- ❑ Other _____

13. What types of resources and/or support would be most helpful in meeting your criminal intelligence training needs? Check all that apply.

- ❑ Train-the-Trainer events/programs
- ❑ Videos/CDs – multimedia presentations
- ❑ Web sites with information on topics of concern
- ❑ Networking opportunities
- ❑ Printed materials
- ❑ Online training
- ❑ Other _____

14. If your organization currently conducts intelligence training, would your organization be willing to provide a copy of your curriculum to assist in developing minimum standards? ❑ Yes ❑ No ❑ NA

Thank you for your assistance. Please return assessment results by May 18, 2004, to:

CITCS Questionnaire
Post Office Box 12729
Tallahassee, Florida 32317-2729
or
Fax to (850) 422-3529
Attention: Michelle Nickens

APPENDIX D

Questionnaire Results

Criminal Intelligence Training Coordination Strategy Questionnaire

Results
June 2004

Introduction

The Criminal Intelligence Training Coordination Strategy (CITCS) Working Group is facilitated through the Counter-Terrorism Training Coordination Working Group (CTTWG) in cooperation with the Global Justice Information Sharing Initiative (Global) Intelligence Working Group (GIWG). The CITCS was established to coordinate intelligence training initiatives in an effort to avoid conflicting messages, to establish and promote mutually agreed-upon intelligence training objectives, and to further the training goals as outlined in the *National Criminal Intelligence Sharing Plan* (NCISP).

The CITCS is organizing an effort to bring together the various organizations developing or offering intelligence training in an atmosphere of coordination, cooperation, goal identification, and resource sharing to address local, state, tribal, and federal criminal intelligence training coordination issues affecting the criminal justice community. The level of commitment and dedication from the members participating in the CITCS demonstrates the importance of intelligence training among our law enforcement community.

Background

The first meeting of the CITCS was held January 8, 2004. Participants were provided an overview of the NCISP with specific emphasis on the core training objectives. A representative from each participating agency described the intelligence training efforts that their agency is planning to develop, currently developing, and/or currently delivering. This roundtable discussion validated that a concerted effort is needed to ensure consistency and coordination when developing intelligence training programs. Breakout sessions were held to identify intelligence training needs. The findings and recommendations were presented to and endorsed by the CTTWG on January 30, 2004.

The second meeting of the CITCS occurred on February 25, 2004. The group participated in breakout sessions tasked to develop minimum training standards for the following five training classifications: Intelligence Analyst, Intelligence Manager, Law Enforcement Officer (In-Service and Basic Recruit), Agency Head/Executive, and Train-the-Trainer. At this meeting, participants suggested conducting an assessment of available training as well as training needs through the use of a questionnaire.

A questionnaire was developed, automated, and distributed to 200 local, state, and federal law enforcement agencies as well as training and intelligence organizations. The questionnaire focused on the types of training offered or being developed, impediments to training, types of

courses/classes offered, and the importance of training for all levels of classification. Submissions were due May 18, 2004. At that time, 58 questionnaires, or 29 percent, were received. Figure 1 summarizes the types of agencies that responded to the questionnaire.

Figure 1

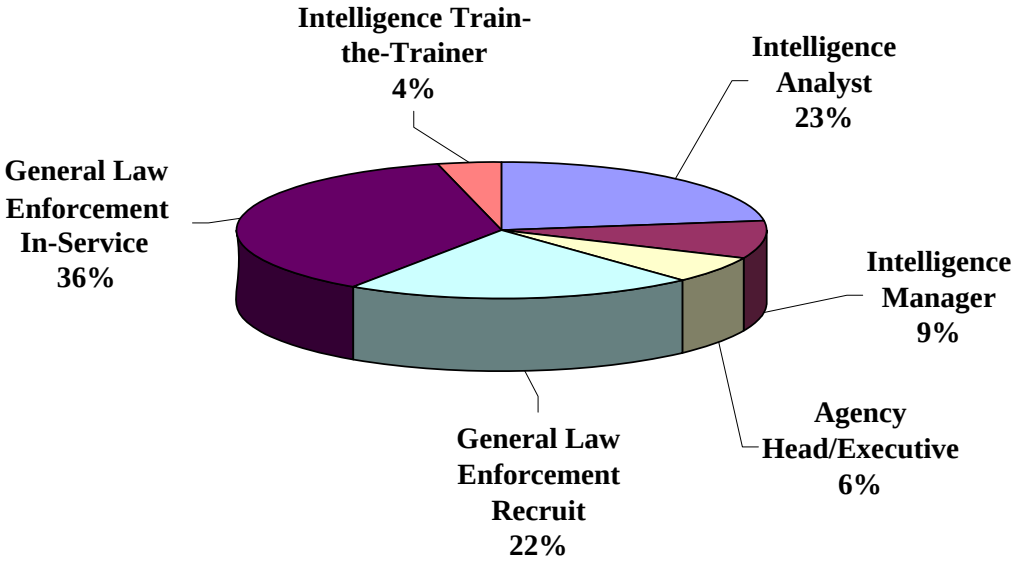
Agency Type	Number of Responses
Local	20
State	24
Federal	5
Other (Training & Intel Centers)	9
TOTAL	58

Questionnaire responses have been aggregated and will not be attributed to a specific agency. Additionally, individual questionnaire results will not be made public. The following analysis summarizes the responses, observations, and findings of the intelligence training questionnaire.

Available Training

First, the questionnaire focused on available training as well as the types of training under development. Based on the number of agencies responding, 60 percent indicated their organization currently delivers criminal intelligence training. Some respondents provide training for multiple training classifications, while others only provide training for one classification, such as Intelligence Analyst. Figure 2 illustrates the percentage of training offered by training classification.

Figure 2



Almost all responding agencies deliver training for the General Law Enforcement In-Service classification, but only 4 percent indicated they provide Intelligence Train-the-Trainer

programs and only 6 percent offer training for Executives. In addition to current programs, the questionnaire asked whether agencies were in the process of developing training for the different training classifications. The majority, 83 percent, indicated that their agency was not in the process of developing training programs or that it was not applicable at this time. However, 17 percent of the respondents are developing training programs. The majority of those responding affirmatively are developing courses for the Intelligence Analyst and General Law Enforcement In-Service classifications. Figure 3 provides a summary of the number of initiatives currently under way by training classification.

Figure 3

Training Classification	Number of Current Training Initiatives Under Development
Intelligence Analyst	9
General Law Enforcement In-Service	8
General Law Enforcement Basic Recruit	7
Intelligence Manager	5
Agency Head/Executive	5
Intelligence Train-the-Trainer	5

Training Needs

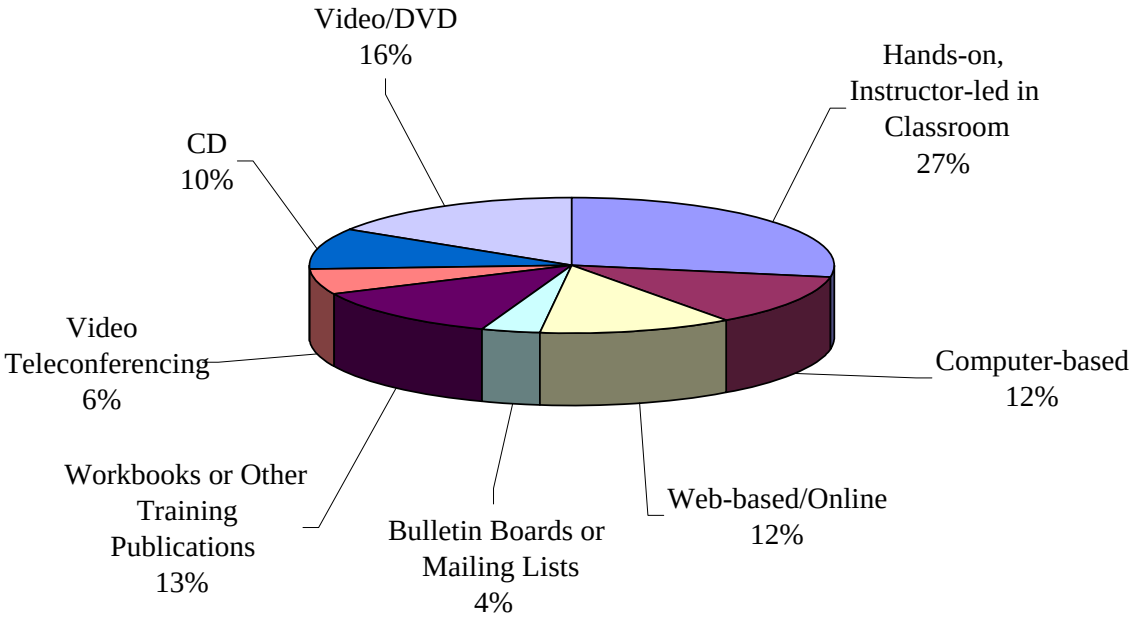
In order to adequately assess what training needs exist and to determine how best to proceed with developing and educating law enforcement agencies on core minimum training standards, the questionnaire asked about the types of training and resources needed.

Questionnaire results indicate that training is lacking in all of the training classifications. However, respondents rated Intelligence Analyst and Intelligence Manager as the classes most lacking in adequate training. Surprisingly, 62 percent of respondents stated they are receiving adequate training, but over a third (36 percent) indicated they were not receiving adequate training. It is important to note, however, that over 72 percent of the respondents who reported that training was adequate currently deliver training programs.

The majority of respondents cited lack of funding as the primary impediment of training, but respondents also rated high on *difficulty finding good trainers, travel and lodging costs*, and *unsure of available training*. Only a handful of respondents selected *unsure of appropriate training for personnel* as an impediment. **One respondent indicated that in order to support the tenets of the NCISP, additional training guidelines and opportunities are needed.** Other respondents indicated that training can be sporadic, which dovetails into the need for core minimum standards that can be used consistently nationwide. Other respondents indicated that their agency has not needed intelligence training because they do not have the staff or resources to engage in an intelligence function.

Respondents were asked to select the method of training delivery most used or preferred. The questionnaire allowed respondents to select as many delivery options as appropriate. Figure 4 indicates that *Hands-on, instructor-led in classroom* method was chosen most often, followed by *Video/DVD*.

Figure 4



One respondent mentioned that on-the-job training can be an effective training tool by assigning personnel intelligence tasks. This concept can further a project or case within the intelligence unit while educating personnel. It is important to note that individuals learn differently, and a combination of these items should be considered when developing training programs.

Lack of resources is commonly cited as an impediment to training. The questionnaire asked agencies to indicate what specific resources are needed to resolve this issue. The majority of respondents said that additional training videos/CDs and multimedia presentations would enhance training for personnel. Agencies also cited networking opportunities as an element for increasing resources and opportunities. All options were selected many times by respondents, perhaps indicating that agencies need resources regardless of what format they are provided—events or formal programs, printed materials, professional association and conferences, or Web sites. Online training was the least selected option. One suggestion was to develop a pool of qualified instructors that agencies or training facilities could call upon when a class is offered. Knowing that these needs exist will assist in developing instructional materials.

Curriculum

This portion of the questionnaire focused on the specific courses or concepts currently being offered by responding agencies. Respondents were provided a basic list of courses and asked to select those that were included in their agency's training programs. The top five courses for each training classification are provided in the left hand column in Figure 5. The right hand column offers other programs not listed in the questionnaire but suggested by respondents.

Figure 5

Intelligence Analyst

Top Five Items Included in Curriculum	Other Suggestions
1-Data Analysis/Link Analysis 2-Intelligence Sharing Systems 3-Intelligence Cycle 4-Introduction to Intelligence 5-Developing Flowcharts	Financial Analysis Money Laundering Telephone Toll Analysis General Intelligence

Intelligence Manager

Top Five Items Included in Curriculum	Other Suggestions
1-Intelligence Sharing Systems 2-Laws, Ethics, Policy 3-Handling/Storing Information 4-Intelligence Purpose/Mission 5-Available Resources	Leadership

Agency Head/Executive

Top Five Items Included in Curriculum	Other Suggestions
1-Legal and Liability Issues 2-Available Resources 3-Intelligence Sharing Networks 4-Leadership Role 5-Intelligence Function and Process	None listed

General Law Enforcement Basic Recruit

Top Five Items Included in Curriculum	Other Suggestions
1-Reporting Procedures 2-Understanding Current Threats 3-Recording and Disseminating Intelligence 4-Legal Limitations/Liability 5-Privacy Issues	28 CFR Part 23

General Law Enforcement In-Service

Top Five Items Included in Curriculum	Other Suggestions
1-Intelligence Sharing Systems 2-Legal Limitations and Liability 3-Privacy Issues 4-Intelligence Cycle 5-Maximizing Intelligence Process	28 CFR Part 23 Trends General Intelligence Leadership

Intelligence Train-the-Trainer

Top Five Items Included in Curriculum	Other Suggestions
1-Intelligence Sharing Systems 2-Topical Materials 3-Legal Basis and Limitations 4-Liability Issues 5-Privacy Issues	Contemporary Issues

These areas may serve as a foundation for developing core minimum training standards. Thirty-four percent of the agencies offering training are willing to share their curriculum to further the development of establishing minimum standards. It is recommended that these agencies be contacted and/or consulted during this development phase.

As mentioned earlier, some respondents believe that training is erratic and inconsistent. Those offering training usually do so annually, although some of the respondents provide training quarterly. By using the minimum training standards along with a diverse delivery strategy, accessibility to quality training should be increased. It is critical that the *right* information is provided to the *right* people in a timely, consistent, and professional manner.

Training Priorities

Questionnaire recipients were asked to rate the importance of establishing minimum training standards for each of the training classifications. All the classifications were rated very high. However, 69 percent of the respondents rated Intelligence Analyst as the most important, followed by Intelligence Manager. Figure 6 provides the rating percentage of each training classification.

Figure 6

	Not Important				*Very Important*
Intelligence Analyst	2%	5%	13%	11%	69%
Intelligence Manager	2%	4%	18%	16%	61%
Agency Head/Executive	0%	12%	30%	21%	37%
General Law Enforcement Basic Recruit	0%	5%	37%	23%	35%
General Law Enforcement In-Service	0%	4%	25%	32%	40%
Intelligence Train-the-Trainer	2%	7%	25%	39%	27%

After providing individual ratings for each of the training classifications, questionnaire recipients were asked to compare the priority level among all the training classifications. Each respondent rated training classifications from 6 (highest priority) to 1 (least priority), using each number only once. Each classification was selected as a top priority by multiple respondents. This exercise validated that all training classifications are critical and require minimum training standards as well as training opportunities.

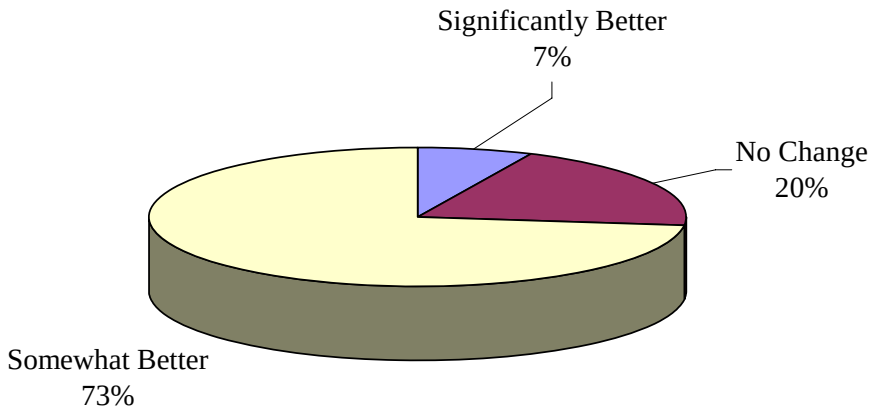
Results from the NCISP Assessment

As part of the GIWG's effort to implement the components of the NCISP, members who attended the December 12, 2003, GIWG Executive Steering Committee meeting requested an assessment tool to be developed to gauge the progress and impact of the NCISP. An assessment tool was developed and disseminated to 217 agencies. A total of 63, or 29 percent, responded. A portion of the NCISP assessment focused on training. The results of these specific questions are included in this document for consideration.

One primary area assessed included changes in opportunities, communications, and resources since the September 11 tragedies. When asked whether training opportunities had increased since September 11, 73.8 percent of the respondents indicated that intelligence training

opportunities were *somewhat better*. Almost 20 percent, however, indicated *no change*. Figure 7 represents the percentage of responses.

Figure 7



NCISP assessment results also included numerous statements from agencies regarding a lack of sufficient training for personnel, including executive and legislative levels. Agencies stressed the need for intelligence training at all levels of law enforcement. One agency recommended establishing training at the basic law enforcement academies and focusing particularly on community-oriented policing efforts. It is important to note, however, that although the comments focused overwhelmingly on the need for more training, 90.2 percent of the respondents indicated their personnel had received intelligence training within the last year. Nonetheless, an overwhelming majority of the respondents cited funding as a primary impediment to enhancing their intelligence function. Lack of personnel, limited training, and inadequate equipment and software were also mentioned.

Conclusion

The CITCS questionnaire confirmed that intelligence training is a critical element in ensuring that the law enforcement community has the appropriate resources and knowledge needed to successfully fulfill their roles and responsibilities. Based on the responses, it is evident that developing minimum intelligence training standards will provide a core baseline for individuals at all levels within their agency as well as at all levels of law enforcement.

All of the training classifications—Intelligence Analyst, Intelligence Manager, Agency Head/Executive, Law Enforcement (In-Service and Basic Recruit), and Train-the-Trainer—are critical components to the overall intelligence function. Each has a unique and intricate role in the intelligence arena and requires adequate and relevant intelligence training.

Observations noted between the CITCS questionnaire and the NCISP assessment are consistent—an increased focus and attention must be aimed at developing minimum training standards, disseminating information and materials to intelligence personnel, and providing increased and enhanced training opportunities.

The information obtained during this process can be incorporated into the CITCS's efforts, as well as in future planning and training programs. The responding agencies recognize the need for intelligence training and minimum standards; their feedback and suggestions will assist in developing standards and possibly in future model curriculum and training programs.

APPENDIX E

Glossary

CRIMINAL INTELLIGENCE

GLOSSARY OF TERMS

NOVEMBER 2004

CRIMINAL INTELLIGENCE
GLOSSARY OF TERMS

The definitions contained herein are provided from the perspective of *criminal intelligence*. 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.

Access (to sensitive or confidential information)—Sensitive or confidential 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 is released to the public 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 that explicit responses to prevent a crime or terrorist attack can be implemented.

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.

Black Chamber—One of the earliest (1919) scientific applications to intelligence that a working group, who was responsible for deciphering codes, used to encrypt communications between foreign powers' diplomatic posts.

C^3—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 certain information be 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* Classification 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.

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.

Cracker—A person who accesses a computer system without consent with the intent to steal, destroy information, disrupt the system, plant a virus, alter the system and/or its processes from the configuration managed by the system manager, or otherwise alter the information in the system.

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 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 Intelligence—*See* Intelligence (Criminal) and Law Enforcement Intelligence.

Criminal Predicate—Information about an individual or his/her behavior that may only be collected and stored in a law enforcement intelligence records system 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 all information in a law enforcement agency's records system is complete, accurate, and secure.

Deconfliction—The process or system used to determine whether multiple law enforcement agencies are investigating the same person or crime and which 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.

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. 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.

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. It can include timelines, event flow analysis, commodity flow analysis, and activity flow analysis. 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 upon 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.

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.

Hacker—A person who has expertise and skills to penetrate computer systems and alter such systems, processes, and/or information/data in files but does no damage and commits no theft or crime. While a hacker may enter files or systems without authorization, the action is more akin to a trespass and no theft or damage results.

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)—A interim conclusion regarding persons, events, and/or commodities based on the accumulation and analysis of intelligence information that is to be proven 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, 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 upon 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 him/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 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 concerning criminal or national security issues. While 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 Records (Files)—Stored information on the activities and associations of individuals, organizations, businesses, and groups who are suspected (reasonable suspicion) of being or having been 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.

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 sworn 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.

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 criminal/fugitives and stolen properties.

Key Word In Context (KWIC)—An automated system that indexes selected key words which represent the evidence or information being stored.

Joint Regional Information Exchange System (JRIES)—A subscriber-supported analytical and resource system for local, state, and federal law enforcement with an interface to the U.S. Department of Defense that provides secure sensitive but unclassified real-time information with databases, e-mail, media studies, threat reporting, analytic tools, and mapping and imagery tools.

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 or 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.

Malicious Software—Self-contained yet interactive computer programs that, when introduced into a computer, can cause loss of memory, loss of data, or cause erroneous instructions to be given in a computer program.

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 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 which 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 which 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 where 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 where 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/herself, 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 to deprive a person of life, liberty, or property, during the course of the criminal justice process, meet constitutional standards.

Procedures—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 while procedure *directs responses* within those limits.

Profile/Criminal Profile—An investigative technique by which to identify and define the major personality and behavioral characteristics of the criminal offender based upon 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 further access to the records would serve no legitimate government interest.

Qualitative (Methods)—Research methods that collect and analyze information which are 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 which can be counted or placed on a scale of measurement that can be statistically analyzed.

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

Racketeering Influenced Corrupt Organization (RICO) 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.

Reasonable Grounds/Suspicion—When a police officer, based upon his/her experience, has an articulable reason to believe that a person or group has committed, is committing, or is about to commit a crime.

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 System (RISS)™—RISS is comprised of six regional intelligence centers that provide secure communications, information sharing resources, and investigative support to combat multijurisdictional crime and terrorist threats to nearly 6,800 local, state, tribal, and federal member law enforcement agencies in all fifty states, the District of Columbia, U.S. territories, Australia, Canada and England.

Regional Intelligence Centers—Multijurisdiction 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 which are operating in or interacting with the region.

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

Reporting—Depending upon 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 if 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, impact and calculate risk; can be qualitative, 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.

SCI (Sensitive Compartmented Information)—Classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems established by the director of the Central Intelligence Agency.

SCIF (Sensitive Compartmented Information Facility)—An accredited area, room, group of rooms, buildings, or an installation where SCI may be stored, used, discussed, and/or processed.

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 which 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 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, which 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 which 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 (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.