CRIMINAL INTELLIGENCE MANAGEMENT:
LEIU's Standards and Recommendations
ASSOCIATION OF LAW ENFORCEMENT INTELLIGENCE UNITS
2019 EDITION
# TABLE OF CONTENTS

Introduction ........................................................................................................... 1
Publication History ................................................................................................. 3
Introduction to the Handbook ............................................................................... 4
LEIU’s Criminal Intelligence Standards ............................................................... 5
Recommendations ................................................................................................. 7

Part 1 - Fundamental Issues ............................................................................. 9
  * Historical Perspective .................................................................................... 9
  * Value of Criminal Intelligence .................................................................. 12
  * Internal Considerations ............................................................................. 13
  * Legal Issues ................................................................................................. 14
  * Political Implications ................................................................................. 15
  * Summary ..................................................................................................... 15

Part 2 - Overview of the Criminal Intelligence Process .................................. 17
  1. Direction and Planning ............................................................................. 17
  2. Collection ................................................................................................ 18
  3. Evaluation and Collation ......................................................................... 18
  4. Analysis .................................................................................................... 18
  5. Dissemination ......................................................................................... 18
  6. Feedback and Re-evaluation ................................................................... 19

Part 3 - Establishing An “Intelligence Capability” ................................................. 20
  * Smaller Agencies ....................................................................................... 20
  * Medium-sized and Larger Agencies ............................................................ 21
  * Training Standards .................................................................................... 23
  * Fusion Centers .......................................................................................... 24
  * Terrorism Liaison Officers (TLO) ............................................................... 24
  * Nationwide SAR Initiative (NSI) ................................................................. 25
Joint Terrorism Task Forces (JTTF) ........................................... 25
Networking and Mutual Aid Agreements ................................ 25
10 Steps for Establishing a Successful Criminal Intelligence Unit. 26

Part 4 - Organizing The Criminal Intelligence Function .......... 28
The Criminal Intelligence Function in Local Law Enforcement... 28
Organizational Structure ...................................................... 28
The Role of the Chief Executive Officer (CEO) ...................... 29
Development of a Mission Statement .................................... 30
Criminal Intelligence Officer’s Mission ............................... 31
Criminal Intelligence Analyst’s Mission ................................ 32

Part 5 - Management And Operations ................................. 33
Management Guidelines ..................................................... 33
Unit Size ........................................................................... 33
Selection of Personnel ......................................................... 34
The Question of Rotation .................................................... 35
Sworn Officers vs Civilians .................................................. 35
Information Gathering .......................................................... 36
Importance of Analysis ......................................................... 40
Automation ........................................................................ 41
Technology Considerations ................................................ 42
Evaluation of the Criminal Intelligence Function .................. 42
Informal Evaluations .............................................................. 43
Formal Evaluations ............................................................... 44

Part 6 - The Criminal Intelligence File .................................. 45
File .................................................................................... 45
File Policies ........................................................................ 45
File Criteria ........................................................................ 46
File Parts ............................................................................ 46
Information Evaluation ................................................................. 48
Classification ............................................................................... 48
Dissemination ............................................................................... 49
File and Information Security ..................................................... 49
Purging and Destruction .............................................................. 49
Part 7 - Criminal Intelligence Briefings ..................................... 51
The Recipient .............................................................................. 51
Briefing Format ............................................................................ 51
Length of the Briefing ................................................................. 52
Written and Oral Briefings ......................................................... 52
Appendices .................................................................................. 54
Appendix A .................................................................................. 55
Appendix B .................................................................................. 57
Appendix C .................................................................................. 59
Appendix D .................................................................................. 62
Appendix E .................................................................................. 63
Bibliography ............................................................................... 68
INTRODUCTION

In 1986, I was two years out of college and ready to take on the world. With degrees in Political Science and Business Administration, and a “gap year” behind me, I was ready for law school. Little did I know, a request from a friend (who also happened to be the police chief) would lead to 32-years in public service.

From 1986 to 1990, the seed was planted, my career began in a 3-officer police department with a city population of approximately 1,600 people. In one shift, you might go from assisting an elderly resident in finding their way home; provide traffic enforcement through the city limits; break up a fight at the local bar; work a vehicle wreck; investigate a burglary at the local farm supply store; or work a homicide at the local convenience store after a robbery. For most of this work, you would either be by yourself, or maybe work with a county deputy or state trooper if one happened to be near you. Regardless, you learned quickly how to process information and to communicate.

Those development years are what led me to understand the value of training and the value of information. I use the term information, because at that time, that’s exactly what I thought it was, just information to help me do my job better. What I did not know at the time, was the way we collected, analyzed, processed, and utilized information was truly “intelligence” and our 3-officer department had a very good “criminal intelligence capability.”

My career has allowed me to work in a wide variety of public safety positions, as a police officer in the 3-officer department, to the State Attorney General’s office and now in the State Highway Patrol with over 2,300 employees. I have served as an intelligence unit supervisor, a fusion center director and participated on numerous committees regarding information and criminal intelligence.

The individuals involved in the early creation of this handbook truly understood information and the value that criminal intelligence brings to a law enforcement agency. I tip my hat as a sign of gratitude to those individuals that helped develop the original handbook in 1988, and for those that assisted with the revisions in 1998, and certainly to the LEIU Executive Board Members involved in this latest revision in 2018. I’m
proud to say that Richard “Dick” Wright, LEIU’s Past General Chairperson has been involved in all three publications and brings a knowledge and passion second to none.

My hope is that this publication can reach the new officer in the 3-officer department as well as the Chief, Sheriff or Colonel in charge of departments with thousands of officers and help them understand and appreciate the value of information and having a criminal intelligence capability. As recommended in the National Criminal Intelligence Sharing Plan (NCISP) developed after the tragic events of September 11, 2001, that every agency, regardless of size, has a stake in the development and sharing of criminal intelligence. All law enforcement can and should be a part of the intelligence process, thereby improving the safety of the nation and its citizens.

Van Godsey, General Chairperson
Association of Law Enforcement Intelligence Units (LEIU)
PUBLICATION HISTORY

In 1987, the Organized Crime Committee of the California Peace Officers’ Association (CPOA) elected to undertake the production of a handbook that would provide direction to smaller agencies in the use and handing of criminal intelligence. The Committee named five command-level law enforcement personnel from several California agencies to produce the manual. The authors included: Michael McMullen, Lieutenant, Palm Springs Police Department; Jack Morris, Administrator, California Department of Justice; Gary Petersen, Captain, Newport Beach Police Department; Gregory Stock, Captain, Santa Barbara Police Department and Richard Wright, Captain, Simi Valley Police Department. On May 18, 1988, their completed manuscript, titled, Criminal Intelligence Program for the Smaller Agency was submitted and subsequently published by the CPOA.

CPOA’s Organized Crime Committee discussed the issue again in 1997. It was decided to revisit the publication and bring it up to date. The revision committee included: Bob Morehouse, Administrator, California Department of Justice; Ken Reid, Investigator, Stanislaus County District Attorney’s Office; Thomas J. Scheidecker, Chief, Ripon Police Department and Richard Wright, Captain, Simi Valley Police Department. The revised manuscript was completed and published by CPOA in 1998.

In 2016, The Executive Board of the Association of Law Enforcement Intelligence Units (LEIU) discussed providing criminal intelligence guidance to law enforcement agencies of all sizes. Since the Criminal Intelligence Program for the Smaller Agency publication had not been available for many years, CPOA was contacted and agreed to relinquish their publication rights to LEIU so that the handbook could be updated to include the various changes in the criminal intelligence arena since the tragedy of September 11, 2001. An LEIU publication committee was formed to revise the booklet. It consisted of: Keith Burt, Deputy District Attorney (Ret), San Diego District Attorney’s Office; Bryan Costigan, Security Director, Montana Lottery; Aaron Kustermann, Chief of Intelligence, Illinois State Police; Bob Morehouse, LEIU’s Executive Director; William Roche, Sergeant, St. Louis (MO) County Police and Richard Wright, LEIU’s Past General Chairperson. Thus, this current version of the booklet, now titled, Criminal Intelligence Management: LEIU’s Standards and Recommendations is being made available to interested readers.
INTRODUCTION TO THE HANDBOOK

Criminal Intelligence is the ultimate management tool for law enforcement. Its use allows agencies to be proactive regarding crime in their community and to address pertinent issues when they are just developing and require less resources to resolve. It is a straightforward “process” designed to facilitate decision-making and crime prevention. The intelligence “process” begins with an identified crime-related issue, a subsequent effort to collect and analyze pertinent information, and the appropriate dissemination to authorized recipients.

This handbook is designed so that law enforcement personnel will recognize the need for a criminal intelligence “capability” within their agency and an understanding of the intelligence “process.” Additionally, it provides appropriate standards and recommendations to ensure the successful operation of a criminal intelligence unit. From this publication, it is hoped that agency personnel may:

- Better assess the need for a criminal intelligence function,
- Determine the size of the agency’s commitment,
- Provide the appropriate direction for the criminal intelligence function, and
- Recognize available resources and organizations that can assist agencies with intelligence issues.

After reviewing this handbook, readers will have been exposed to a number of viable criminal intelligence options. Based upon an agency’s size and staffing, a basic issue is whether to add a criminal intelligence “capability” or a complete intelligence unit. Other considerations include; the manner in which the function will operate, its incorporation within the organization, personnel selection, specific mission, and whether to join a network in partnership with other agencies. Throughout the handbook, an effort has been made to describe the organizational benefits derived from the proper use of the criminal intelligence process.

Any questions related to this publication or the criminal intelligence function may be directed to LEIU’s staff at: LEIU@doj.ca.gov

The Editors
LEIU’S CRIMINAL INTELLIGENCE STANDARDS

LEIU considers these Standards as a prerequisite for establishing and managing a successful and legitimate criminal intelligence function. Law enforcement agencies are invited to adopt the Standards for their own use.

**Direction and Control**
- The agency’s Chief Executive Officer (CEO) has ultimate responsibility for the criminal intelligence function.
- The CEO shall establish the criminal intelligence function, determine the mission and provide appropriate direction and resources.
- Policies and procedures that address criminal intelligence operations and establish Constitutional safeguards shall be implemented and enforced.
- Properly trained staff, including an analyst, should be assigned.
- Evaluation of the intelligence function should be conducted on a periodic basis to ensure compliance and the ability to meet designated goals and objectives.

**Collection**
- Criminal Intelligence information shall be collected and stored in a lawful manner and in compliance with Constitutional rights, federal and state laws and local regulations.
- Criminal Intelligence file content shall be limited to information which indicates that there is “reasonable suspicion” that the subject or group is involved, or is suspected of being involved, with known or suspected criminal activity.
- Criminal intelligence information should be evaluated for mission relevance, source reliability and content validity prior to submission to file.

**Maintenance**
- The criminal intelligence file, either a hard copy or electronic file, shall be maintained in a secure manner, with access controlled by assigned personnel. The file shall be separate from other types of agency files.
- LEIU File Guidelines or Federal Regulation 28 CFR Part 23 should be used for intelligence file maintenance.
Subject information in the file shall be re-evaluated within five years from the submission or previous update. Information found to be no longer current, accurate, or relevant to the agency’s mission shall be purged. In order to extend the retention period, any updates require reasonable suspicion of continuing criminal activity.

**Dissemination**

- Dissemination of criminal intelligence shall be for lawful purposes only.
- Dissemination of criminal intelligence shall be on a “need to know” and “right to know” basis.
- Accurate record keeping of the date, nature and purpose of each dissemination of criminal intelligence information is required. The record keeping shall include the individual’s name, title and name of the law enforcement agency to which the disclosure was made.
- Criminal intelligence information obtained from an outside agency shall not be disseminated to a third party without authorization from the originating agency.
RECOMMENDATIONS

In addition to LEIU’s Criminal Intelligence Standards, the following specific recommendations are provided to assist law enforcement personnel involved with the criminal intelligence function. A detailed discussion of each recommendation can be found on the pages indicated below.

1. The Criminal Intelligence Unit’s mission must be clearly stated and shared throughout the organization. (Page 13)

2. Each criminal intelligence unit should establish and maintain an ongoing working relationship with an attorney well versed in the intelligence function. (Page 14)

3. The criminal intelligence officer will immediately advise appropriate personnel when a criminal situation involving a public figure becomes known. (Page 15)

4. The jurisdiction’s executive officer and elected officials should be advised of the presence and purpose of the criminal intelligence function. (Page 15)

5. All law enforcement officers should be trained to understand the criminal intelligence process and their role in properly reporting suspicious activity related to crime or terrorism. (Page 23)

6. The highest priority should be placed on acquiring initial training and refresher courses in criminal intelligence for assigned staff, those in the chain of command and the unit’s legal advisor. (Page 23)

7. The CEO should strongly consider participating in a criminal intelligence network with neighboring agencies and a regional intelligence center. (Page 25)
8. The criminal intelligence officer or supervisor should meet with the CEO on a regular basis; and have direct access when the need arises. (Page 28)

9. The unit's mission should be focused on specific criminal activities. (Page 30)

10. The criminal intelligence unit’s staff and resources must match the size and scope of the described mission. (Page 30)

11. Absent exigent circumstances, a full-time criminal intelligence officer should be excluded from any direct enforcement activities. (Page 31)

12. Policies and procedures must be established to ensure appropriate accountability for unit operations, file control, informant control, special funds and security. (Page 33)

13. Due to the requirements of this specialized assignment, criminal intelligence officers should not be subject to mandatory rotation. (Page 35)

14. If the budget permits, the intelligence unit should be staffed with a combination of a sworn officer(s) and a civilian analyst(s). (Page 35)

15. Informant Development training should be mandatory for all sworn criminal intelligence personnel. (Page 38)
PART 1

FUNDAMENTAL ISSUES

The Chief Executive Officer (CEO) making the decision regarding implementation of a Criminal Intelligence function should recognize the issues such units have encountered in the past. The following description of selected historical events is by no means exhaustive and is offered only as guidance to the reader.

Historical Perspective

Law enforcement agencies across the United States in the 1970s and 1980s and occasionally since then have experienced negative publicity and lawsuits because of improperly managed criminal intelligence units. The identified problems stemmed from operating without appropriate guidelines. The involved agencies had collected and stored intelligence information improperly, stored non-crime related information and focused investigations on non-criminal organizations or individuals.

A brief historical overview is required to understand how this situation developed and how it has changed. In the late 1960s, when the domestic tranquility of the United States was under siege by subversive organizations and widespread riots, many law enforcement agencies responded by using undercover officers to infiltrate suspected groups to obtain information on suspicious individuals and their organizations. This information was subsequently placed in criminal intelligence files. Law enforcement’s efforts were obviously designed to alleviate the criminal behavior and help settle the unrest that was sweeping the country. However, there were no guidelines or criminal intelligence standards in place to balance law enforcement’s need for information versus an individual’s right to privacy. At the time, there had only been one Supreme Court case which had upheld the concept of the “right to privacy” (Griswold vs. Connecticut, 381 U.S. 479 (1965)). This case decision related specifically to marital privacy, but over the subsequent years court decisions and legislative actions have expanded individual privacy rights on a more general basis.
The events of the early 1970s, including the ongoing dissension over the
war in Vietnam, the Watergate scandal and the publicity surrounding the
FBI’s COINTELPRO (Counter Intelligence Program), aggravated a
growing distrust of government by some segments of society. Aggrieved
individuals and civil liberties organizations subsequently filed numerous
lawsuits against law enforcement agencies for violating individual privacy
rights while accumulating criminal intelligence.

The efforts to professionalize and standardize law enforcement
Commission on Criminal Justice Standards and Goals published a book,
titled Report on Police, which addressed law enforcement’s functions,
including intelligence. This publication set operational standards and
made a number of recommendations.

By the mid-1970s, the Association of Law Enforcement Intelligence Units
(LEIU) along with the California Department of Justice, the New Jersey
State Police and the Federal Bureau of Investigation had established
standards for intelligence files. These standards addressed individual
privacy rights related to the collection, maintenance and dissemination of
criminal intelligence.

The 1970s additionally saw the creation of the Regional Information
Sharing System (RISS). By 1983, RISS had established six regional
centers across the country serving local, state, tribal and federal law
enforcement agencies (Appendix E). These centers helped develop an
intelligence capability that complied with generally accepted guidelines

The International Association of Law Enforcement Intelligence Analysts
(IALEIA) was established in 1981. This organization focused on
advancing high standards for intelligence analysis and has been
instrumental in training, certificating, and professionalizing the field
(Appendix E).

As a result of a New Mexico lawsuit settled in 1993, civil libertarians, led
by the American Civil Liberties Union and the National Lawyers Guild,
accepted LEIU’s Criminal Intelligence File Guidelines (Part 6) as a
standard for law enforcement agencies involved with criminal
intelligence. This agreement established the accepted balance between the
needs of law enforcement and an individual’s privacy rights.
The terrorist attacks of September 11, 2001, identified the need for improved information sharing within the law enforcement community. Subsequent federal legislation brought changes to intelligence efforts across the country. Of primary importance to law enforcement efforts was the adoption of the *National Criminal Intelligence Sharing Plan (NCISP)* (*Version 1.0 in 2003 and Version 2.0 in 2013*). This plan made numerous recommendations and provided training standards and implementation guidelines for local, state, tribal and federal law enforcement agencies involved in criminal intelligence. It specifically highlighted the need for sharing intelligence products (Appendix C).

The post 9-11 Congressional investigations and the 9-11 Commission Report led to the *Intelligence Reform and Terrorism Prevention Act of 2004*. This Act established the Office of the Director of National Intelligence (ODNI) (*www.dni.gov*) which was designed to coordinate the efforts of all federal intelligence organizations. This Act also provided legislative intent to establish locally controlled information systems where potential terrorism-related information could be contributed by law enforcement agencies for analysis to determine emerging trends. Following this guidance, the *Nationwide Suspicious Activity Reporting (SAR) Initiative* was implemented (*https://nsi.ncirc.gov*).

Shortly afterwards, a national network of fusion centers was established to collect, evaluate, analyze and disseminate intelligence information to local agencies in a specific geographic area. These centers are located in every state and most major urban areas (Appendix E).

As a result of these advancements, a collaborative information sharing environment now exists for law enforcement agencies that choose to participate. With appropriate guidelines in place, law enforcement agencies with a professionally managed intelligence unit can now operate without being overly concerned about the threat of adverse litigation.
Value of Criminal Intelligence

A properly managed criminal intelligence unit provides law enforcement administrators with advanced knowledge for the development of strategic and tactical plans that best utilize agency resources. In essence, criminal intelligence provides situational awareness and is focused on proactive crime prevention. This allows the agency to deal with specific crime issues when they are small and can be managed with minimal resources.

The primary function of a criminal intelligence unit is to provide credible information and analysis to various members of the agency. The CEO and administrators benefit from strategic products while patrol officers, investigators and jail personnel benefit from tactical products and officer safety information.

A criminal intelligence unit has many products to offer. They include:

**Strategic Products**

- Community reports assessing crime problems
- Reports on trends and projections for planning, budgeting and resource allocation
- Reports on current crime trends and their locations (e.g. support for hot-spot policing)
- Recommendations on crime targets, policy and legislation
- Threat assessments for local events and individuals (crime, traffic, terrorism, etc.)
- Reports on criminal enterprise development
  - Nature and characteristics
  - Participants, organizations and businesses
  - Intentions and capabilities
  - Strengths and weaknesses
  - Structure and methodology
**Tactical Products**

- Assistance to enforcement units
  - Graphical displays
  - Descriptions of criminal associations and locations
  - Investigative packages on people, organizations, or locations
  - Officer safety alerts and bulletins
  - Support to criminal investigations
- Community crime alerts
- Private sector/business collaboration

**Internal Considerations**

A smaller agency, unable to afford more than one full-time Criminal Intelligence Unit staff member, can benefit as much as a larger agency with many people. The basic approach is the same and the skills needed are identical. The intelligence needs of the CEO operating either a large or a small agency, must remain similarly proactive to avoid future criminal activity. The success of the unit will ultimately depend upon the creation, implementation and management of appropriate policies and procedures.

Agency management is enhanced as the criminal intelligence expertise is developed and begins to allow the CEO to use the unit as an early warning system regarding anticipated criminal activity. When the decision is made to implement a criminal intelligence function in the agency, it is incumbent upon the CEO to impart to its staff a strong sense of mission.

**Recommendation 1**

*The Criminal Intelligence Unit’s mission must be clearly stated and shared throughout the organization.*

The perception of the Criminal Intelligence Unit has been an issue with some agencies. In many instances, the mission of the unit is not clear to others in the agency. The function, role, objectives and the mission of the unit must be well known to others within the organization. Successful criminal intelligence units require the support of other agency personnel to ensure that pertinent information is forwarded to them. The established guidelines for the release of information from the unit and the alteration of the traditional organizational structure should be explained to avoid misconceptions about the unit.
Legal Issues

Recommendation 2

Each criminal intelligence unit should establish and maintain an ongoing working relationship with an attorney well versed in the intelligence function.

Every agency with a criminal intelligence function should have access to legal assistance familiar with intelligence issues. Legal issues related to intelligence differ from criminal law and the required legal expertise is not always available in the local City Prosecutor’s or District Attorney’s office. The legal standard for including information in a criminal intelligence file is “reasonable suspicion” (Appendix A) which is a lower standard than “probable cause” and requires different rules to protect the privacy of information regarding individuals and organizations which may be included in the file.

In the United States, intelligence-related law and regulation is found at all levels, beginning with Constitutional privacy and association rights to federal, state and local statutes. A designated attorney must be familiar with the various statutes relating to the concerned jurisdiction since statutes tend to differ among states and local jurisdictions. The attorney should also understand the agency’s intelligence policies so timely responses to legal requests can be addressed.

The need for such legal assistance has diminished in recent decades for those agencies that have professionalized their operation with appropriate training and management. However, modern technology continues to raise legal issues regarding privacy rights and access to personal information maintained by government agencies. It is important for an agency to establish policies related to the use of drones, public demonstrations, surveillance, record retention/dissemination, and social media since they are all related to the intelligence function. Thus, agencies need to ensure the responsible attorney is properly trained in the applicable laws that impact the jurisdiction and the agency’s policies related to criminal intelligence.
Political Implications

Recommendation 3
The criminal intelligence officer will immediately advise appropriate personnel when a criminal situation involving a public figure becomes known.

The CEO and members of the Criminal Intelligence Unit should be sensitive to the possible political implications of some criminal intelligence. Such information should be brought to the CEO in a timely manner for appropriate consideration.

Recommendation 4
The jurisdiction’s executive officer and elected officials should be advised of the presence and purpose of the criminal intelligence function.

The operational characteristics of the Criminal Intelligence Unit, which includes guarded files, information based on “reasonable suspicion”, unique targets, and the like, can be viewed by some as a "spy" operation. This may be countered by a continuing educational process in which the CEO ensures that all concerned are aware of the duties, responsibilities and the benefits of the criminal intelligence function. This educational process must go beyond the agency’s personnel and should include the city/county administrators, elected officials and the public.

City or county administrators and elected officials are ultimately responsible to the community for the services of their governments, and therefore must be fully cognizant of the unit and the legal constraints under which the unit operates.

Summary

A properly directed Criminal Intelligence Unit, while working within specified guidelines, can produce a considerable amount of information. This information must be in such quality and quantity and with such timing, that it allows the CEO to effectively deploy resources to successfully curtail criminal operations.
The key to the success of this unit is the level of interest paid to it by the CEO. A commitment must be made by the CEO to ensure intelligence operations are legal, goal oriented and properly managed.
PART 2

OVERVIEW OF THE CRIMINAL INTELLIGENCE PROCESS

The criminal intelligence process is a cycle of activity composed of several pronounced steps. Each activity in the cycle depicted below is designed to be completed before the next activity is undertaken. The criminal intelligence process can be a lengthy one, or one requiring little time to complete. Much of the time required relates to the depth of the raw data being examined and the skill of the reviewer.

The criminal intelligence process is divided into six primary parts: direction and planning, collection, evaluation and collation, analysis, dissemination and feedback and re-evaluation.

1. Direction and Planning

Direction and planning starts with the agency’s CEO who has the responsibility for establishing the criminal intelligence function, determining the unit’s mission, setting priorities and providing appropriate direction and resources. More specific planning is the responsibility of the unit manager/supervisor who assigns individual intelligence projects.
2. **Collection**

The next step in the process is the accumulation of raw data needed for a specific intelligence product. This effort requires a “Collection Plan” which should be coordinated between the unit supervisor, an analyst and the assigned collector(s). The Collection Plan should identify the assigned personnel, the information being sought, the methods and resources required to obtain the information and an appropriate timeline for completion. The information needs to be collected in a lawful manner from any number of possible sources. Those sources could include; citizens, criminal informants, public documents, department records, electronic intercepts, an investigator’s observations or the internet.

3. **Evaluation and Collation**

Evaluation involves reviewing the raw data for possible inclusion in the intelligence file. This appraisal would include determining the reliability of the source and the validity of the information. The reviewer also decides whether the information complies with department guidelines regarding the unit’s mission and has the required criminal nexus.

Collation involves merging, indexing, and filing the newly received criminal intelligence with the information already contained in the files.

4. **Analysis**

Analysis is the part of the intelligence process that transforms the raw data into a useful product. It involves compiling, summarizing, comparing and organizing data within the file to provide a more complete picture of a designated criminal issue. Thus, it transforms information into actionable intelligence.

5. **Dissemination**

Dissemination is the timely sharing of criminal intelligence with a consumer who has a “right to know” and a “need to know.” It is an important step since criminal intelligence is of no value
unless it is provided to those who can legitimately use it to prevent crime or increase public safety.

6. **Feedback and Re-evaluation**

The final step of the process requires feedback from the consumer regarding the product produced by the intelligence process. This step allows for a proper evaluation and a determination of whether there needs to be any modification to improve the product or the effectiveness of the intelligence function.
PART 3

ESTABLISHING AN “INTELLIGENCE CAPABILITY”

In 2003 and again in 2013, the National Criminal Intelligence Sharing Plan (NCISP) issued recommendations. Among them was, “Every law enforcement agency should have an intelligence capability. Agencies participating in the intelligence process, regardless of their level of participation, stand to gain considerable value and significantly improve their crime-reduction efforts. Participation may be as basic as the simple collection and sharing of information with a nearby fusion center or task force, combined with the receipt of future intelligence products from that entity that can be shared with appropriate agency personnel.”

Today the prevailing threat of terrorist activity along with cybercrime and the sophistication of organized criminal groups requires law enforcement agencies to collect and share pertinent criminal information. Modern policing philosophies such as Community Oriented Policing (COP), Compstat, Intelligence–Led Policing and Predictive Policing all rely upon the process of collecting, analyzing and disseminating crime-related information to help prevent crime and enhance community safety. The question becomes to what extent can individual agencies participate in this effort?

**Smaller Agencies**

The vast majority of law enforcement agencies in the U.S. are small, have limited staff and historically have not participated in the criminal intelligence process. However, it has become apparent that all law enforcement agencies should be actively engaged in at least the “collection and reporting” responsibilities of the criminal intelligence process. Since most of the law enforcement agencies across the country are small it is important those agencies train their personnel so they can participate in properly reporting suspicious criminal information or possible terrorist activity to an intelligence operation.

There is significant value for an agency to share pertinent crime or terrorism-related information with adjoining agencies and a regional intelligence center. Crime or terrorism does not recognize jurisdictional
borders, so suspicious activity in one community may be a small but important part of a regional problem.

**Medium-sized and Larger Agencies**

In 1973, the *Report on Police* published by the National Advisory Commission on Criminal Justice Standards and Goals set standards pertaining to law enforcement’s criminal intelligence operations. Standard 9.11 stated, “Every police agency with more than 75 sworn personnel should have a “full-time” criminal intelligence capability.”

Today, this standard is still recommended. With the advent of professional standards and innovative technology, the criminal intelligence function has become an essential management tool that helps maintain a safe community. Medium-sized and larger agencies need a properly staffed full-time intelligence unit. The actual size of the staff and the assigned mission should reflect the specific needs of the concerned jurisdiction.

Medium-sized agencies have on occasion found it difficult to maintain appropriate staffing within a criminal intelligence unit given competing personnel demands. Sometimes these agencies have assigned unit personnel other non-intelligence related tasks or temporary reassignments when staffing vacancies occur in operational units. Typically, this can be counterproductive since a properly managed intelligence unit reduces the need for more operational staff by addressing crime problems proactively and recommending solutions that addresses problems when they are small and require less resources. Unfortunately, if an officer is diverted from the intelligence function the process begins to slow significantly, particularly when only a few individuals (including both clerical and sworn) are responsible for the entire collection and processing system. The intelligence process requires constant attention to maintain a proactive posture, and to ensure the files are updated and accurate. The maintenance of the files is important as the deterioration of the system can cause legal implications for the involved agency.
Another issue for intelligence units involves having access to an intelligence analyst. The intelligence process requires analysis, so those units without an analyst should contribute their raw information to a regional intelligence center or fusion center for processing and analysis. Some medium-sized agencies that wish to keep the intelligence process in-house have addressed this issue by cross-training their crime analysts as intelligence analysts. This effort can prove to be both efficient and cost effective; but should include specific training on the intelligence process as the focus between the two assignments is different.

Crime analysts normally focus on crimes against persons and property and deal with crimes that have already occurred while looking for trends and series. They identify the presence and scope of specific crime problems. Intelligence analysts deal in crimes that are typically conspiratorial in nature. These analysts paint the picture of who and why, while assisting in the preemption, disruption and prevention of crime.

Larger agencies, with over 250 sworn and diverse populations, should ensure that their resources provide access to information concerning criminal activity in each of the communities within their jurisdiction. In the United States, many immigrants reside with their own ethnic groups in enclaves where they speak their own native language, maintain their own cultures and tend to distrust American law enforcement. This distrust is usually based upon their experience in their former countries and extends to the point that community members may not inform law enforcement of ongoing criminal activity. In many cases, these same groups have an organized crime component that tends to victimize their own people. This type of situation requires the intelligence unit to include an officer or have access to a reliable source that speaks the language and understands the culture in order to learn of any criminal activity.

The 1973 Report on Police, which was commissioned by the Law Enforcement Assistance Administration (LEAA), incorporated survey results from numerous police chiefs. Some of the recommendations for major cities included in Standard 9.11 were:

- The number of personnel assigned should be based on local conditions.
- The intelligence operation should be centralized; however, intelligence specialists may be assigned, where appropriate, to major transportation centers.
• The intelligence operation should include an independent and well-secured reporting and record system.

**Training Standards**

**Recommendation 5**

All law enforcement officers should be trained to understand the criminal intelligence process and their role in properly reporting suspicious activity related to crime or terrorism.

All sworn law enforcement personnel should be trained in the fundamentals of criminal intelligence, either in the basic academy or through in-service training. At a minimum, this would include being able to understand their role in the intelligence process and the proper means for reporting pertinent information to a local or regional intelligence center.

The National Criminal Intelligence Sharing Plan indicated the “Core Training Objectives” for all law enforcement officers are:

- To understand the criminal intelligence process and its ability to enhance their contributions to the criminal justice system.
- To be provided with information on available data systems, networks and resources.
- To be able to identify key signs of criminal activity and the procedures for collecting data and reporting such activity.
- To gain an understanding of the legal, privacy and ethical limitations placed on the collection of criminal intelligence information.

**Recommendation 6**

The highest priority should be placed on acquiring initial training and refresher courses in criminal intelligence for assigned staff, those in the chain of command and the unit’s legal advisor.
Personnel assigned to the intelligence function require more extensive training to fulfill their assigned responsibilities. The agency’s training commitment for intelligence should also include the CEO, those in the chain of command and the unit’s legal advisor. *The National Criminal Intelligence Sharing Plan* identified specific training standards for all levels of law enforcement personnel involved in the criminal intelligence process (Appendix C). A master calendar for training opportunities is available at the National Criminal Intelligence Resource Center’s website [http://mastercalendar.ncirc.gov](http://mastercalendar.ncirc.gov).

LEIU and the International Association of Law Enforcement Intelligence Analysts (IALEIA) annually host a training seminar that features renowned speakers and numerous workshops involving intelligence topics. This event usually draws 600-700 attendees and provides an opportunity to meet and network with other intelligence professionals (Appendix C).

LEIU and IALEIA also offer a training course for those involved in the intelligence function entitled, Foundations of Intelligence Analysis Training (FIAT). This is a 40 hour course held 15-20 times at various locations in the U.S. and Canada each year (Appendix C).

**Fusion Centers**

Many law enforcement agencies, both large and small, have joined fusion centers in their vicinity. Fusion centers are described as “primary focal points within a state or local environment for the receipt, analysis, gathering and sharing of threat-related information among federal, state, local, and territorial partners.” They conduct analysis and facilitate information sharing, assisting law enforcement and homeland security partners in preventing and responding to crime and terrorism. They are owned and operated by state and local entities with support from federal partners (Appendix E).

**Terrorism Liaison Officers (TLO)**

Most fusion centers around the country have established Terrorism Liaison Officer(s) (TLO) positions. Sometimes these positions are titled Fusion Liaison Officers (FLO) or Intelligence Liaison Officers (ILO). Law enforcement agencies participating in a regional fusion center may appoint one or more of their officers to attend training and become liaisons
to the intelligence center. These officers then facilitate the exchange of pertinent information between their agency and the intelligence center.

**Nationwide SAR Initiative (NSI)**

The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) is a “collaborative effort by the U.S. Department of Homeland Security, the Federal Bureau of Investigation, and state, local, tribal, and territorial law enforcement partners. This initiative provides law enforcement with a tool to help prevent terrorism and other related criminal activity by establishing a national capacity for gathering, documenting, processing, analyzing and sharing SAR information. The NSI defines suspicious activity as observed behavior reasonably indicative of pre-operational planning associated with terrorism or other criminal activity.” ([https://nsi.ncirc.gov](https://nsi.ncirc.gov)). Most fusion centers serve as the collection point for SARs within their area of responsibility. Fusion centers process the information provided and share it with all appropriate agencies.

**Joint Terrorism Task Forces (JTTF)**

Another option for law enforcement agencies is to assign personnel to their regional Joint Terrorism Task Force. There are 104 such task forces located in 71 regions across the United States. These task forces comprise a partnership between various federal, state and local law enforcement agencies in a multi-agency effort led by the FBI that is designed to combat terrorism (Appendix E).

**Networking and Mutual Aid Agreements**

**Recommendation 7**

_The CEO should strongly consider participating in a criminal intelligence network with neighboring agencies and a regional intelligence center._

A viable option for reducing the intelligence workload for a small or medium-sized agency is to participate in a networking or mutual aid criminal intelligence agreement. These agreements can be either formal or informal, with any number of surrounding law enforcement jurisdictions. Conceivably, neighboring agencies have common crime problems which can be approached with shared resources. This type of task force concept allows an agency to assign limited personnel to work
with intelligence officers from surrounding jurisdictions on combined investigations (Appendix D contains a networking outline).

These task forces provide sufficient staffing to conduct interviews and surveillances without disrupting the normal activities of other units within the involved departments. It also ensures cooperative sharing of criminal intelligence within a specific area concerned with common threats.

The task force arrangement can be expanded to the point where one lead agency within a region maintains the responsibility for keeping the intelligence files while other member agencies provide the investigative personnel. Member agencies would have access to the files for both input and dissemination purposes. This type of agreement would be similar to several large-scale intelligence networks such as the RISS Projects or fusion centers.

The pooling of resources from several agencies is also a tremendous asset in training new or inexperienced criminal intelligence officers. Criminal intelligence is a specialized area of law enforcement which requires considerable exposure and training prior to an officer gaining an appropriate level of expertise. Thus, networking would allow new criminal intelligence officers the opportunity to work with experienced personnel while they gain an understanding of this unique aspect of law enforcement.

An additional benefit to this type of arrangement would be that individual departments do not lose all their criminal intelligence expertise if an officer retires, promotes, or transfers from the criminal intelligence position. Instead, there is a pool of expertise to service the combined areas.

10 Steps for Establishing a Successful Criminal Intelligence Unit

1. Create a proper environment:
   - Obtain the active support of the Agency’s CEO.
   - Gain the political and budgetary support from appropriate elected officials.
   - Educate the agency and the community concerning the benefits of having a criminal intelligence function.
2. Establish the criminal intelligence unit as a proactive crime prevention operation that supports the concept of Community Oriented Policing (COP).

3. Design a unit mission statement focused toward specific criminal activities and disseminate it to the entire agency.

4. Select qualified personnel, including a trained analyst, to staff the unit.

5. Obtain separate, secure quarters for the unit.

6. Implement and enforce professional guidelines for:
   - Unit operations
   - File procedures
   - Security
   - Special expense funds
   - Informant control

7. Provide training for:
   - The CEO
   - Appropriate elected officials
   - Criminal Intelligence managers and supervisors
   - Criminal Intelligence officers and analysts
   - The remainder of the Agency’s personnel
   - Legal advisor

8. Liaison with neighboring agencies and participate with the local or state fusion center. Join the Association of Law Enforcement Intelligence Units (LEIU).

9. Require both strategic and tactical products from the unit and evaluate its operations on a regular basis.

10. Ensure the CEO meets regularly with the criminal intelligence unit supervisor to provide appropriate direction.
PART 4

ORGANIZING THE CRIMINAL INTELLIGENCE FUNCTION

The Criminal Intelligence Function in Local Law Enforcement

Law enforcement criminal intelligence is a proactive crime prevention function that involves an information collection and analysis process conducted to support the anticipated need for decision making and action.

Organizational Structure

Recommendation 8

The criminal intelligence officer or supervisor should meet with the CEO on a regular basis; and have direct access when the need arises.

The criminal intelligence function in a law enforcement agency is a separate and distinct activity which requires special consideration when placing it within the department’s structure. The criminal intelligence officer or a unit supervisor, depending on the size of the unit, should have direct access to the CEO. This direct access is imperative since the unit’s primary function is to provide the CEO with timely, strategic criminal intelligence, which will allow for planning to meet developing criminal trends. Frequently, in agencies which assign only one or two officers to the criminal intelligence function, the routine supervisory duties such as timekeeping and evaluations, may be assigned to a supervisor who is also responsible for other units. These supervisors must recognize the need for the intelligence officer to report directly to the CEO. This reporting procedure, which circumvents the normal chain of command, is used to eliminate communication filters and to ensure the confidentiality of criminal intelligence information.

Ideally, the Criminal Intelligence Unit should be located in its own access controlled and securable office with appropriate security protections for the intelligence file system. It should not be combined with other units such as narcotics, vice, detectives, records or internal affairs.
Criminal intelligence files are distinctly different from routine investigative files and other law enforcement records since criminal intelligence is based upon the legal standard of “reasonable suspicion.” Information from these files is regulated by different laws and procedures; including purge, retention and access requirements. Criminal intelligence information must be disseminated on a “need to know” and “right to know” basis. It is information which is commonly described as proactive, crime prevention oriented and not designed for court use.

**The Role of the Chief Executive Officer (CEO)**

The CEO of a law enforcement agency has critical responsibilities regarding the intelligence function. A starting point for understanding this role would be to initially review the National Criminal Intelligence Sharing Plan (NCISP) (Versions 1.0 & 2.0). This plan was endorsed in 2003 by U.S. Attorney General John Ashcroft and the U.S. Department of Justice and includes model policies, standards and guidelines for developing a local law enforcement intelligence function. It provides recommendations for implementation issues and methods for sharing critical information.

Once the function is initiated, the CEO specifically needs to accept his/her role and responsibilities in producing the strategic and tactical products that will enhance public safety. Those responsibilities include establishing the intelligence unit’s mission, setting its priorities and providing ongoing direction and support. Additionally, the CEO will need to ensure that the function has the active support of the whole department and the necessary resources to accomplish its mission. And finally, the CEO has an obligation to appropriately act on the recommendations that are the product of finished intelligence.

An issue for the CEO is the need for community support for the intelligence function. Criminal intelligence is a subject that should be explained to the public by the CEO and/or upper management. The public should understand the criminal intelligence process is a legitimate crime prevention tool requiring their participation to prevent crime and create a safer community.
**Development of a Mission Statement**

The Criminal Intelligence function, like other specialized law enforcement assignments, requires appropriate direction and focus. Specific parameters are necessary so the criminal intelligence effort will not lose its perspective, and will retain its ability to consistently deliver a useful product. Mission statements help provide direction and must clearly state the organization’s expectations of its Criminal Intelligence Unit.

Mission statements should concisely address three essential components:

1. The first portion of the mission statement should describe the criminal intelligence process of collecting, evaluating, collating, analyzing and disseminating information related to criminal activities.

   **Recommendation 9**

   *The unit's mission should be focused on specific criminal activities.*

2. The second component of the mission statement requires the agency to identify the type or scope of criminal activity on which the Criminal Intelligence Unit has been directed to focus. In crafting this portion of the statement, it is important to determine what crime problems or issues are specifically threatening the jurisdiction. Each community or geographic area has its own unique challenges and the mission statement should reflect those concerns. For example, if a jurisdiction’s prevailing crime problem involves criminal street gangs or “emerging organized crime groups,” then the mission statement should identify those issues as the unit’s focus.

   **Recommendation 10**

   *The Criminal Intelligence Unit’s staff and resources must match the size and scope of the described mission.*

It is also critical to identify an objective that can realistically be accomplished by the personnel and resources assigned to the unit. It is counterproductive to design the mission in such broad terms that the assigned personnel cannot adequately perform their job.
Therefore, it is important the unit’s resources match the size and scope of its described mission.

3. The final portion of the mission statement should describe the results which are expected to be obtained by the unit. Since the primary function of the Criminal Intelligence Unit is to provide strategic intelligence or long term planning recommendations to the CEO, this portion of the mission statement should indicate that the information provided will allow the CEO to make rational choices regarding unanticipated criminal threats and the deployment of the agency's resources.

The following is a "sample" mission statement:

"The Department's Criminal Intelligence Unit will collect, evaluate, collate, analyze and disseminate information on individuals and groups who are suspected of being involved in (criminal problems of concern to the jurisdiction) and will provide this information to the CEO for crime prevention and decision making purposes."

A properly worded mission statement will provide needed direction for the personnel assigned to the unit and will allow the remainder of the department and interested reviewers to understand the function and purpose of the Criminal Intelligence Unit. This knowledge will also allow others to recognize that they can assist the Criminal Intelligence Unit by being the "eyes and ears" that contribute information which can help enhance their community's crime prevention efforts.

**Criminal Intelligence Officer’s Mission**

**Recommendation 11**

Absent exigent circumstances, a full-time criminal intelligence officer should be excluded from any direct enforcement activities.

The intelligence officer's primary mission is to provide sufficient information and appropriate lead time to the CEO so future criminal activity may be thwarted. A full-time intelligence officer is primarily an information gatherer and should not be placed in an enforcement role.
requiring court testimony. This role would not preclude an officer from taking appropriate enforcement action in exigent circumstances. The general exclusion from direct enforcement is due to the nature of the information collected and the privacy rights of the involved subject(s).

The duties assigned to an intelligence officer differ depending upon the size and responsibilities of the unit. In a small one or two-person unit, the responsibilities could include everything from the administrative maintenance of the file to the field activities of collecting raw information. In larger units, with administrative staff, the duties would usually be directed towards information collection, threat assessment and liaison with other agencies.

**Criminal Intelligence Analyst’s Mission**

The *National Criminal Intelligence Sharing Plan* describes the mission of an intelligence analyst, “is to research and analyze raw data, apply critical thinking and logic skills to develop sound conclusions and recommendations, and provide actionable intelligence in a cohesive and clear manner to management.”

In order to perform this mission some of the desired characteristics of an analyst would include: initiative, good judgement, communication skills, research ability, computer skills, the ability to plan and prioritize and knowledge of current events.
PART 5
MANAGEMENT AND OPERATIONS

Management Guidelines

Recommendation 12
Policies and procedures must be established to ensure appropriate accountability for unit operations, file control, informant control, special funds and security.

It should be recognized that criminal intelligence is a management intensive function. As part of the establishment of a Criminal Intelligence Unit, management must clearly define the mission and the principles under which the department expects the unit to operate. These policies should include a clear statement the department has a prohibition against the use of illegal or unauthorized methods of obtaining or distributing criminal intelligence. Management has the overall responsibility for ensuring unit personnel comply with established policies and procedures.

Management of the function needs to include periodic evaluations and the insistence on routine housekeeping duties. These duties include documentation of informant management, special funds and compliance with the unit's guidelines regarding file retention, dissemination and purging criteria.

Unit Size

Once a Criminal Intelligence Unit is established, the CEO needs to determine the number of personnel that can be committed to the function. The unit's size should depend upon the size and needs of the organization. The recommended minimum size would be one full-time position with no collateral duties.

- The assigned officer would need to devote a considerable amount of time to the administrative function of maintaining the files in a legal manner.
- To be effective, the criminal intelligence officer would need to maintain effective liaison with other agencies and the regional intelligence center.
Cultivating reliable sources of information is a time-consuming task. Only through well-placed sources and a thorough knowledge of open sources of information can a criminal intelligence officer begin to provide management with appropriate insight into identifying developing problems in the community.

If a department can devote more than one full time position to the criminal intelligence function an increase in production should result. The second position should incorporate the skills of an analyst. This capability will significantly enhance the unit's ability to present quality information to the CEO.

There may be some CEOs in smaller agencies who wish to devote only a part-time effort to the criminal intelligence function. Although this is not recommended, it may be the only course available. In this situation, the assigned individual’s mission should be very narrowly focused and the primary function should involve collecting and reporting pertinent information to a regional intelligence center for processing and dissemination.

**Selection of Personnel**

The key to optimum performance in the intelligence unit is its personnel. Strict selection criteria must be set to increase the likelihood of the unit’s success. Intelligence personnel should possess the following essential characteristics:

- Integrity
- A strong commitment to the goals of the agency
- Imagination and resourcefulness
- High intellectual capability and analytical ability
- The ability to communicate effectively in written and verbal form

While these are a few of the characteristics which are important, the criminal intelligence officer must also possess a high degree of maturity and be able to work without supervision while initiating and successfully completing assignments. Another consideration is the ability to establish rapport with diverse individuals, from law enforcement personnel to the various members of the community. This ability is crucial and will ultimately determine an officer’s capability to obtain information from a
wide range of sources. Other important characteristics are an officer’s judgment and his ability to anticipate what may occur in any given situation. Obviously, there are many individual skills to consider, but the success of the unit ultimately will depend on the talents of the assigned personnel.

The Question of Rotation

Recommendation 13
Due to the requirements of this specialized assignment, criminal intelligence officers should not be subject to mandatory rotation.

Any personnel selection process would be remiss without some comment or consideration of a rotation policy for unit personnel. There are two schools of thought concerning the rotation of personnel from one assignment to another. Some would recommend that unit members be rotated on a regular basis, while others believe that individuals should be left in an assignment if they are productive and meet organizational goals. There are several reasons to support the retention of experienced individuals in the criminal intelligence function. These reasons include: knowledge of the intelligence process and crime subject; strong contacts among other intelligence officers; and the training investment and skill development.

Sworn Officers vs Civilians

Recommendation 14
If the budget permits, the intelligence unit should be staffed with a combination of a sworn officer(s) and a civilian analyst(s).

Consideration should be given to the partial civilianization of criminal intelligence position(s). Civilianization may offer several benefits, not the least of which is a solution to the inherent problem of the intelligence officer being promoted and assigned elsewhere. Although the use of either sworn officers or civilians can provide a unit certain benefits, neither are without issues. A traditional, action oriented police officer may find the intelligence function of gathering information not as challenging or exciting as street police work and may lose interest in the position. Conversely, a civilian does not have some traditional information mechanisms, such as informants, available for the collection process and may be limited in obtaining confidential information. However, many
civilians bring other attributes to the unit such as formal education in research and analytical methods. These qualities are critical to the intelligence process.

Many agencies already employ civilians as analysts in other capacities. These same individuals can often be cross trained and utilized for the criminal intelligence function. Civilians are sometimes considered outsiders in the police world, and a few may find it difficult to gain acceptance into certain law enforcement agencies. The acceptance problem is not unique to the field of criminal intelligence, even for sworn personnel, and is normally overcome as the staff member gains credibility. If staffing permits, the blending of civilian and sworn will have positive aspects for both positions and thus the problems of rotation and acceptance are reduced.

**Information Gathering**

Once a specific intelligence project is identified, the planning for the methods and procedures for the collection of information must be considered and implemented. This “Collection Plan” is important. If a proper plan is not devised and carried out, then the objective is frequently not obtained. Criminal intelligence personnel can be deployed in various ways depending upon the project. They can be assigned by criminal suspect, criminal organization, geographic area, organized crime type or by specific criminal activity. The decision usually depends on the type of information gathering effort being undertaken.

Data can be gathered through or from surveillance, undercover operatives, electronic data sources, criminal informants or citizen sources. A method which should not be ignored is the use of overt intelligence personnel being assigned to monitor known criminal suspects and their public meeting places. Once the habits of these subjects are established, intelligence officers can create appropriate opportunities to observe or converse with the criminal subject in public places. This type of consensual contact can be very effective. Many times, criminal subjects will willingly converse with police investigators in public. This interaction can provide investigators with valuable insight into the personal traits and capabilities of the involved subject. Even those subjects who will not voluntarily speak with known intelligence officers can be influenced by observing the officers in public places where the subject expects to conduct either social or business meetings with criminal
associates. The psychological impact of this type of contact in restaurants, bars, hotels and other public places may impede the subject’s illegal activity and make them concerned that the officers are aware of their criminal intentions.

In addition to specific intelligence projects that are undertaken by the unit, regular sources of information must be cultivated and established by the unit to keep abreast of criminal activities within the jurisdiction. This stream of information would also include the review of selected crime and arrest reports, newspaper articles, search warrants, special publications and items from law enforcement contacts or community sources.

A valuable resource for personnel assigned to criminal intelligence efforts is the ability to individually network with others in the intelligence field. Personal contacts provide the basis for building trusted relationships and allows for sharing information with others that have common interests. LEIU assists with networking efforts by providing members with a roster of other members that list the agency, an individual’s specialty assignment and contact information. Additionally, LEIU and IALEIA’s annual training seminar provides an opportunity to interact with knowledgeable contacts that have or may be facing similar intelligence challenges.

Intelligence gathering efforts will occasionally produce specific crime-related information that does not meet mission requirements and should not be considered for inclusion in the intelligence file. However, this raw information may be useful to other units within the agency and should be appropriately referred to the proper unit.
1. **Human Intelligence (HUMINT)**

Human intelligence is gathered by communicating with those individuals who may be in a position to provide pertinent information regarding background information or specific information on the subject(s) of the project. This type of effort is one of the best ways to ensure the information is current and accurate as the officer can often determine the original source of the information, the sources’ motivation for providing the information and the relationship to the concerned subject. Individual sources or informants contributing intelligence can be used or accessed either overtly, covertly or a combination of both. Criminal intelligence can be obtained through controlling and directing informants; or allowing for information to be obtained without supervision.

**Recommendation 15**

**Informant Development training should be mandated for all sworn criminal intelligence personnel.**

There are three distinct types of informants. Each is important and should be used in the criminal intelligence function.

1. **Citizen Informant:** Any non-law enforcement person whose life style is not characteristic of criminal activity.
2. **Officer Informant:** Any law enforcement officer.
3. **Criminal Informant:** An individual whose lifestyle, either through criminal record or association, is characteristic of criminal activity.

All criminal intelligence officers are encouraged to develop worthwhile, productive informants. In addition to the paid or criminal type informant, many persons not directly involved in criminal activities may have information of value to the mission of the criminal intelligence unit. Both types should be developed on an ongoing basis.
Because the use of informants is such a vital but precarious law enforcement function, training in the development and use of informants must be mandatory. The Criminal Intelligence Unit must establish written guidelines regarding the use of informants. Proper documentation should be kept establishing the informant’s identity and motive for assisting law enforcement. Records should also be maintained describing the type and validity of information received and an accounting of monies paid for services rendered. Informant handlers and supervisors should seek to corroborate information from informants.

Officers must guard against developing personal relationships with informants which are social or could otherwise cast doubt on their integrity during informant contacts. They must recognize that informants are department resources, and the officers are only temporary managers of those resources.

2. **Physical Surveillance**

Criminal intelligence officers frequently use covert surveillances in their work. Covert physical surveillance is described as the observation of suspected criminals, meetings or locations without the knowledge of the target. Purposes for surveillance of a suspected criminal subject are to discover associates, places visited, vehicles or transportation methods, and activities engaged in by the subject being observed. Purposes for conducting surveillances of meeting locations (or locations of suspected criminal activity) may include, determining persons or vehicles present, schedule of meetings and obtaining size of a criminal group. Surveillances may involve stationary, foot, vehicular, aerial and electronic means by the involved officers. Since many criminals are sensitive to the probability of being observed, surveillance operations normally require several officers in order to be conducted without detection.

Properly conducted surveillances require not only appropriate vehicles and equipment, but also significant preparation and planning. Effective physical surveillance requires practice, patience, proper communications and coordination between the involved officers. It is recommended that newly assigned criminal
intelligence officers receive appropriate training in surveillance techniques.

3. **Specialized Equipment**

Surveillance activities may require specialized equipment. Some agencies own all or some of this equipment and others may need to borrow from other agencies. There are regional resources for loan through the Regional Information Sharing Systems (RISS), the local High Intensity Drug Trafficking Area (HIDTA), local counter narcotics task forces, or other specialized work units (Appendix E).

Some of the specialized equipment used for surveillance include: cameras, audio and video recording systems, vehicle tracking systems, binoculars, night vision and other items. Depending upon state laws and local regulations, the use of some of these items may be restricted or prohibited.

**Importance of Analysis**

The importance of the analysis phase in the operation of the criminal intelligence function cannot be overstated. Analysis of information is the “heart” of the criminal intelligence process and turns information into actionable intelligence. In the strategic environment, analysis helps produce reports which draw conclusions and makes recommendations that allow a manager or a CEO to take appropriate action to deploy or re-deploy personnel, assign budget priorities, create investigative bodies or to prevent or reduce crime. In the tactical environment, it can assist in officer safety, target selection or in solving crimes. It may also assist prosecutors when they go to court. Thus, the analysis phase of the process is of critical importance to the end product.
**Automation**

The last few decades have produced technology which has had a significant impact on law enforcement and the criminal intelligence function. These advances in automation have provided numerous tools that can be used to support the various phases in the intelligence process.

- **Collection / Searches**
  
  A long-standing challenge for intelligence professionals is the search for information. As illustrated in other portions of this guide, there are numerous sources of valuable information. Internet sources include both commercial and government databases. Searching these various locations can be a time-consuming endeavor. Advancements in information technology has provided solutions for searching these systems. For example, a user can now enter a name, date of birth, social security number, and phone number to send a query to multiple systems at the same time.

- **Analysis**
  
  Analysis can also be a time-consuming process. In addition, sharing the processes used by analysts and intelligence officers can be difficult. Information technology tools now allow intelligence professionals to save their analytical processes, track progress on a project, allow others to work collaboratively on an issue and save the steps or tradecraft so successful steps can be shared and repeated. Most firms supplying these services charge per-person and after configuration costs, single licenses can be affordable for smaller organizations.

- **Common Operational Picture or Situational Awareness**
  
  Some intelligence units are tasked with providing a common operational picture or what is also called situational awareness to public safety executives or incident commanders. There are currently tools available to automate some of this process. Visualizing where undercover officers are during a major event, tracking suspicious events and many other elements can be displayed using a single image. This type of service can be a valuable tool for decision-makers and supervisors alike.
• **Dissemination and Briefings**

There are several tools available to brief executives and aid in tracking dissemination of intelligence products. Some of these technologies will send a unique version of each document shared with a large list. This can be useful as a security system to ensure each person receiving the information is handling the information appropriately. Additionally, there are some tools which can create intuitive briefing materials for executives which allows these materials to be continuously updated. These tools have the benefit of providing a professional looking format and save significant time.

**Technology Considerations**

The decision by management to employ any modern technology to enhance their criminal intelligence function depends on several factors. First, it is important to recognize the scope of what is expected from the criminal intelligence unit and to consider which tools would be most useful. Second, cost is a factor and this entails the initial purchase price as well as required training and ongoing maintenance. Third, decisions regarding information security and the interoperability of any selected technology with other agency systems must be considered. Additional information on automation may be obtained by contacting the LEIU’s Executive Board at leiu@doj.ca.gov.

**Evaluation of the Criminal Intelligence Function**

For many years, there was a popular perception that the evaluation of criminal intelligence operations was difficult, if not impossible. It is now recognized evaluation is attainable either informally or formally.

1. **Reasons for Evaluating**

   Regardless of the motive behind the demand for accountability, all law enforcement services should be ready to provide proof of their worth. It is good business to prepare for the expected demands and it is wise to know what the underlying questions are likely to be. A few questions regarding the criminal intelligence function could be:
a. Have the end products been valuable?
b. Can these end products be obtained elsewhere?
c. Should the staff be used elsewhere?

Without a long-term evaluation program and past compilations to review, the criminal intelligence officer can have a difficult time answering these questions.

2. **Benefits of Evaluation**

Periodic evaluations tend to demonstrate if the function is meeting its stated objectives. They also assist in developing future plans based upon the documented past.

3. **Types of Evaluation**

Sometimes an organization’s efforts in evaluating their Criminal Intelligence Unit are more confusing and cumbersome than necessary. Formal and extensive evaluations are not always necessary and in many situations, simple answers to pertinent questions will provide the information needed regarding the status of a unit. Using the answers to the questions in the “Chief Executive’s Eyeball Evaluation” (Appendix B) may eliminate the need of having to spend an inordinate amount of time in more complex evaluations.

The following information provides some insight into both informal and formal types of evaluations:

**Informal Evaluations**

An informal evaluation is as the name implies: lightly done, but focused enough to depict what must be known. It does not rely upon rigid collection forms and time frames for success. Rather, to be successful, it only uses stated objectives, an accounting of end results and an inspection of the file system.

As a start, this suggestion calls for the development of several written objectives acknowledged by the CEO, the unit commander and the criminal intelligence officer. When the staff member meets a stated objective, it is considered a job completed in a satisfactory manner. It is
important to remember all objectives must be quantifiable. However, the CEO must be reasonable with the expectations to ensure quantity does not overshadow quality.

A log might be maintained during the year documenting the production of end products together with titles, dates and the resulting use by the agency and others in the law enforcement community. Some of the end products include: briefings made, reports written, training delivered, special compositions for task force use and others. Some of this accounting is written down when work starts and concludes. Other accounting is acquired by calling recipients who benefitted from the work, and inquiring about how the end products were used.

More now than in the past, criminal intelligence files have become the center of much attention by criminal intelligence personnel. It is inside this all-important data bank that a great amount of accounting can take place. In fact, the file may be equal in importance to the objectives and end products. This is because the use of the file deals with the right to privacy, dissemination, audit trails, file size and purging. A brief audit trail can document the size of the file at the start of a reporting period, its change in size by the end and determine how the file materials were used.

**Formal Evaluations**

Agencies who want to treat the evaluation of the criminal intelligence operation in the most comprehensive manner possible, may use the formal approach. This approach calls for the greatest amount of time and supervisory commitment. This means setting in place reporting and collecting procedures, training personnel in their compilation, review, analysis and then using the resulting information in the management of the criminal intelligence function.
PART 6
THE CRIMINAL INTELLIGENCE FILE

Every criminal intelligence program which has existed for more than a few days has some form of file. The assembled data may be stored in a highly sophisticated and computerized manner or thrown together as a bundle of paper in a shoe box. Whatever it is called, it remains a file. A file must have certain qualities for it to become useful, dependable and reliable as a database. The following subject areas offer some suggestions for file structure.

File

The file is designed to provide the agency with a sound database of information which is used to legitimately meet identified needs, for carrying out its mandate of protecting the public and suppressing criminal planning and operations. By definition, the file is an information storage and retrieval system that includes indices, forms and controls.

File Policies

Management must clearly define the areas in which the Criminal Intelligence Unit will operate and define the parameters of that definition. Criminal intelligence consists of stored information on the activities and associations of:

1. Individuals who:
   - are suspected of being, or having been involved in the actual or attempted planning, organizing, financing or commission of criminal acts, or
   - are suspected of being, or of having been involved in criminal activities with known or suspected crime figures.

2. Organizations, businesses and groups that:
   - are suspected of being, or of having been involved in the actual or attempted planning, organizing, financing or commission of criminal activities, or
   - are suspected of being, or of having been illegally operated, controlled, financed or infiltrated by known or suspected crime figures.
Only information with a criminal predicate meeting the agency's criteria for file input should be stored in the criminal intelligence file. Non-criminal information that is purely political, sexual, racial, religious, or is composed of personal beliefs and preferences of individuals and groups is unacceptable as criminal intelligence data. However, the above described information can become acceptable when the information is crime related and incidental to one of the department approved crime categories assigned to the Criminal Intelligence Unit. It is recommended either the LEIU File Guidelines or the Code of Federal Regulations, Title 28, Part 23 (28 CFR Part 23) should be used to manage intelligence files. A complete copy of LEIU’s File Guidelines may be obtained by a request to LEIU at leiu@doj.ca.gov.

The decision as to whether public records and confidential information are kept in separate files is a management decision. Criminal Offender Record Information (CORI), however, should be excluded from the file because it may be subject to audits and dissemination restrictions separate from criminal intelligence files. Additionally, if information is contained in other files and is readily accessible by the criminal intelligence unit personnel it is not necessary to duplicate the information in the criminal intelligence file.

**File Criteria**

Setting file criteria means defining what crime categories will be stored in the file (e.g. organized crime, criminal extremists, emerging crime groups, etc.). These criteria will vary among agencies because of unique crime problems, geographical area and available resources.

**File Parts**

There are three parts of the filing system: working, temporary, and permanent.
1. **Working**

All newly arrived data is thought to be in the working phase, so long as it has not been indexed. This phase allows time for inspecting the new data regarding acceptability for functional use and indexing. Anything rejected is either destroyed or routed to another recipient whose mission includes the new data. Accepted data is classified as either temporary or permanent and made a part of the unit's files. Generally, the information in your working files should not be disseminated until it is evaluated and contains the requisite reasonable suspicion of a criminal predicate.

2. **Temporary**

New data that has been accepted for filing during the working phase is reviewed for quality. Should the material be desirable, but lack in one or more important identifiers or other pertinent data, it is assigned temporary status. It is common for many large and small intelligence operations to allow up to one year in the temporary category before requiring a review to see if the information should be made permanent, purged, or retained for another year in temporary status. However, any information indexed into the criminal intelligence file, even if marked temporary, must contain a reasonable suspicion for a criminal predicate.

3. **Permanent**

New data, or data classified as temporary, is upgraded to permanent status when the subject of the information has been positively identified and all the other qualities of a permanent file are met (e.g. accuracy, crime and mission related).
**Information Evaluation**

All raw data received for file consideration must undergo a rigorous review before acceptance into the system. Among the considerations are the following:

- Is it crime related?
- Is it mission related?
- Is it verified?
- How reliable is the source?
- How valid is the material?

The first three considerations can be achieved quickly by scanning the newly arrived material. When the answer is "yes" to all three questions, the material will probably be accepted for filing. The last two questions can be documented by using the following table or something similar:

<table>
<thead>
<tr>
<th>SOURCE</th>
<th>MATERIAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Reliable</td>
<td>1. Confirmed</td>
</tr>
<tr>
<td>B. Usually Reliable</td>
<td>2. Probable</td>
</tr>
<tr>
<td>C. Unreliable</td>
<td>3. Doubtful</td>
</tr>
<tr>
<td>D. Unknown</td>
<td>4. Cannot be judged</td>
</tr>
</tbody>
</table>

**Classification**

Many agencies realize the importance of a uniform classification system when they share information. It becomes abundantly clear that one agency's classification of secret, restricted, and public is nearly impossible to relate to others without a uniform classification system. The following four classifications are recommended for use by the Criminal Intelligence Unit: **Sensitive, Confidential, Restricted, and Unclassified**.

1. **Sensitive** is the highest possible security. Access is limited to only those whose names appear upon the route slip. Usually this includes the Unit supervisor/manager and those above him/her in the chain of command.

2. **Confidential** is a medium security level. Access is limited to intelligence personnel only.
3. **Restricted** is the lowest level of security. Access is limited to law enforcement personnel.

4. **Unclassified** is public information.

**Dissemination**

Criminal intelligence information maintained in the unit's files should only be released to requesters on a right-to-know and need-to-know basis. Right-to-know is defined as the official capacity and statutory authority for the requesting individual or agency to receive the requested information. Need-to-know is defined as the requirement that the information requested is both pertinent and necessary for the requesting individual or agency to initiate, further, or complete an assigned law enforcement task. All information shared with any person outside of the Criminal Intelligence Unit should be routinely documented.

No “original document” which has been obtained from an outside agency is to be released to a third agency. Should such a request be received, the requesting agency will be referred to the submitting agency for further assistance.

**File and Information Security**

Security is the essence of criminal intelligence operations, and good security adds to its credibility. Security includes limited access to the facility and non-access to the files, unless supervised by intelligence personnel. If hard copies of criminal intelligence reports are maintained, the documents should be kept in secure/locked cabinets. Access to electronic systems and files has to be tightly monitored and properly controlled. A resource for best practices for securing electronic data can be located at: [https://www.zdnet.com/article/10-security-best-practice-guidelines-for-consumers](https://www.zdnet.com/article/10-security-best-practice-guidelines-for-consumers).

**Purging and Destruction**

Information may be kept in criminal intelligence files as long as it meets file criteria. Information in the intelligence file is removed and destroyed when it no longer qualifies for retention based on a review to determine its usefulness, timeliness, appropriateness, accuracy and completeness. The review schedule should be pre-determined (generally accepted retention
periods are one year for temporary files and five years for permanent files). Additionally, organizations should make "purging review" part of their daily routine, which means looking at documents for their usefulness each time the files are accessed.

When files are automated, they can usually be programed to provide warnings when files/information are nearing a purge review date (typically this warning will sound 90 days before the purge review/retention date).

Purged documents should be destroyed as quickly as the law or office policy allows. Nothing should remain in a purged file that once identified a person or organization. Agencies need to recognize state law or local ordinances may require that original documents must be retained for a specific time frame prior to destruction. If a criminal intelligence document is removed from a file for purging prior to the minimum standard under the state law or local ordinance, then an appropriate purging procedure needs to be adopted. However, even if units are required to maintain the physical records because of their retention policy, no information should be disseminated from purged files.
The briefing can be delivered as a short document or presented orally. It can also be delivered as an amalgamation of the two. The best possible setting for a briefing includes only a few, but important characteristics. First, the briefing should be developed for a known recipient such as the CEO; or other law enforcement personnel having both a need and a right to the information; second, the format should be as simple as possible. Finally, the briefing should be short and concise.

**The Recipient**

Knowledge of the recipient of the briefing will assist the criminal intelligence personnel to focus the research and guide the level of presentation. When the recipient is not known beforehand, the intelligence personnel may report too broadly in order to cover all possible needs. If the recipient will be the CEO, the briefing should be directed toward his/her needs and not to the desires of other persons who might have been invited to attend by the CEO.

There will also be times when briefings will be given to patrol or detective commanders, and others such as task forces or conference attendees. When these assignments occur, it is important to know the composition of the audience.

**Briefing Format**

The simplest format is often the best. One format that is often used includes four parts:

1. problem statement
2. analysis
3. conclusions
4. recommendations
The first part, *problem statement*, is little more than a one-liner stating why the criminal intelligence presenter has come before the recipient. This short opening remark is important since most CEOs are busy and need to be refreshed as to the purpose of the person’s visit.

Second is the *analysis* portion of the briefing. Here, the presenter provides the facts without personal interpretation. The facts are stated in their natural order of events to aid the recipient in assimilating what must be known.

The *conclusion* portion of the briefing allows the criminal intelligence representative to offer educated analysis as to what the facts mean, and what the target may be conspiring to do next.

Last is the *recommendation* portion of the briefing. The presenter should always have one or more recommendations ready for the CEOs consideration. After all, the criminal intelligence representative is *the expert* on the subject, and should be allowed to have a voice in the discussions.

**Length of the Briefing**

Briefings can either be short or long, depending on the subject matter and the needs of the recipient. However, a typical briefing in which the criminal intelligence representative sets the length, should be short. The purpose of a briefing is to do little more than *alert* those few persons who must know certain things about a specific subject. Since CEOs are often busy, it behooves the criminal intelligence representative to keep remarks both organized and brief. Concise briefings are the key to making the best use of the CEOs time.

Most well organized briefings can be delivered in seven to ten minutes. For many administrators, those few minutes will not be seen as diverting them from their busy schedules.

**Written and Oral Briefings**

When directed to deliver a briefing, the criminal intelligence representative should compose the necessary notes in a manner that can support both written and oral presentations. This would require writing the notes in the same format/order as the verbal briefing.
At the conclusion of a briefing in which a written briefing has been left for the recipient, consideration should be given regarding the paper's confidentiality and maintenance. Controls should be established to ensure the return of the briefing package to the criminal intelligence representative.
## APPENDICES

<table>
<thead>
<tr>
<th>Appendix</th>
<th>Page #</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Glossary of Terms</td>
<td>55</td>
</tr>
<tr>
<td>B. Chief Executive’s “Eyeball” Evaluation</td>
<td>57</td>
</tr>
<tr>
<td>C. Training in Criminal Intelligence</td>
<td>59</td>
</tr>
<tr>
<td>D. Basic Elements of a Network Agreement</td>
<td>62</td>
</tr>
<tr>
<td>E. Criminal Intelligence Organizations and Resources</td>
<td>63</td>
</tr>
</tbody>
</table>
APPENDIX A

GLOSSARY OF TERMS

Classification
A rating given stored information. A classification indicates dissemination restrictions.

Criminal Intelligence
An information collection and analysis process conducted to support the anticipated need for decision-making and action.

Reasonable Suspicion
The legal standard for including information in an intelligence file. “Reasonable suspicion” is established when sufficient facts provide a trained law enforcement officer a basis to believe there is a reasonable possibility an individual or organization is involved in a definable criminal activity or enterprise.

Mission
A description of the unit's goal, mandate, purpose or objective.

Need-to-Know
The information requested is both pertinent and necessary for the requesting individual or agency to initiate, further or complete an assigned law enforcement task.

Right-to-Know
The official capacity and statutory authority for the requesting individual or agency to receive the requested information.

Permanent File
A file containing both confidential and public information on criminal matters relating to the unit's mission and maintained for an extended period.
**Temporary File**
A file containing both confidential and public information into which is placed material requiring more identifiers, or which lacks sufficient verification as to its crime relationship. It is maintained in that state for a limited period.

**Working File**
Raw material newly arrived in the unit that is in a state of initial review before it is indexed and added to the file or destroyed.

**Source Document**
The original document in a file (important to retain when files are automated). At least one source document must also contain the criminal predicate or reasonable suspicion for creating the entry.

**Strategic Intelligence**
Intelligence material that tends to support long range planning.

**Tactical Intelligence**
Intelligence material that tends to assist immediate law enforcement needs and supports short range planning.
APPENDIX B

CHIEF EXECUTIVE’S EYEBALL EVALUATION OF THE CRIMINAL INTELLIGENCE UNIT

Management Questions to Ask the Criminal Intelligence Staff

1. What is the status of the unit/file guidelines?
   a. Are professional guidelines in place?
   b. Are the guidelines being followed?

2. Is the Unit staying within the guidelines?
   a. Crime targeting
   b. Filing, indexing, purging, destruction
   c. Retention periods and audit trails
   d. Appropriate dissemination

3. Is the unit staying within the approved mission?
   a. Should we add or delete authorized crime areas?
   b. Is the mission too broad for the unit’s staffing levels?

4. Is unit training needed?
   a. Informant development, report writing, legal issues
   b. Analytical techniques, internal procedures
   c. Analytical tools and automated techniques

Operational Questions to ask the Criminal Intelligence Staff

1. What is the status of the unit's objectives?
   a. Are the objectives being met?
   b. Should new objectives be set?

2. Is the unit producing both strategic and tactical products?
   a. Are the products useful?
   b. Are the products properly disseminated?
3. Does the unit provide the chief executive with recommendations?
   a. Does the chief executive receive them in time to react?
   b. Do the recommendations prove useful?

4. Does the unit comprehend "right to privacy?"
   a. Are unit personnel aware of "privacy" requirements?
   b. Do unit personnel understand the “need-to-know” and “right-to-know” concepts?
   c. Do unit personnel understand the “3rd Party Rule” of dissemination?

5. Is the unit's file properly managed?
   a. Is new information properly evaluated prior to inclusion in the file?
   b. Are the files updated or purged in a timely manner?
   c. Are security procedures followed?

6. What are the intelligence unit's end products?
   a. Do they relate to proactive crime prevention?
   b. Do they assist the chief executive in his/her decision making?
   c. Are the products accompanied by written analytical reports detailing critical questions, recommendations, and conclusions?

Contributed by: Jack Morris, CA DOJ (Ret.) / Bob Morehouse, LEIU Executive Director
APPENDIX C

TRAINING IN CRIMINAL INTELLIGENCE

The National Criminal Intelligence Sharing Plan (NCISP), Version 1—2003, published by the International Association of Chiefs of Police (IACP) recommended training (Recommendation #18) at all levels for law enforcement personnel involved in the criminal intelligence process. The training standards, as contained within the NCISP, shall be considered the minimum training standards for all affected personnel. Additionally, recipients of criminal intelligence training, as recommended in the NCISP, should be recognized and awarded certificates for successful completion of training.

The report identified several recommendations specific to training issues:

- Training should provide recipients with the skills to provide more targeted, evaluative summary data to decision-makers.
- Appropriate training must be provided to in-service law enforcement personnel and basic recruits on information sharing systems and criminal intelligence concepts.
- Training should promote building trust for intelligence sharing.
- Training should promote protection of civil and constitutional rights.
- Training should emphasize that all personnel, regardless of position, have a role in the intelligence process and information sharing.
- Training should equip personnel to use new technologies. It is important that recognition be given to those individuals and agencies that participate in the training curriculum. Certificates of Completion should be given to each individual who participates in the varied levels of intelligence training by the entity delivering the training.

The NCISP, Version 2 - 2013, stated, “As their environment changes, law enforcement and homeland security officials must meet new challenges head-on. Meeting these challenges requires training, which helps ensure the safety of both the officers in the field and those they serve, while maintaining effective policing strategies. This Version discusses training components and the avenues needed (such as distance-learning platforms) to implement the tenets of the NCISP.”
Getting Started—Training

- Access the National Criminal Intelligence Resource Center to identify training opportunities both online and via the Criminal Intelligence Training Master Calendar available at: http://mastercalendar.ncirc.gov.

- Utilize the standards identified in the Minimum Criminal Intelligence Training Standards when finding training opportunities for law enforcement personnel, including analysts at: https://it.ojp.gov/gist/108/Minimum-Criminal-Intelligence-Training-Standards.

- Additional analytic standards can be accessed at Global Information Sharing at https://it.ojp.gov/GIST/ under the titles of Minimum Standards for Intermediate-Level Analytic Training Courses; and Common Competencies for State, Local, and Tribal Intelligence Analysts.

- Incorporate basic training on intelligence into in-service training.

Additional Training Opportunities:

- **Foundations of Intelligence Analysis Training (FIAT)**

LEIU, in conjunction with the International Association of Law Enforcement Intelligence Analysts (IALEIA) provides training entitled FIAT, which stands for Foundations of Intelligence Analysis Training. This training is provided all over the U.S. and Canada—usually 15-20 times a year. Contact the Central Coordinating Agency (CCA) of LEIU at LEIU@doj.ca.gov for available training schedules or visit the LEIU webpage at www.leiu.org and click on “Training” near the top of the page.
• **Annual Criminal Intelligence Training Seminar**

LEIU—in conjunction with IALEIA—hosts an annual week-long training event (held across the U.S. and Canada in different locations). This training event has internationally recognized speakers and leaders in the intelligence community on hand to provide up-to-date information. Speakers and workshops involve training related to criminal intelligence, international terrorism, criminal intelligence management and supervision, topics that relate to organized crime and gangs, and information sharing among law enforcement. The training event also has three certificated tracks for “Fundamentals in Criminal Intelligence”, “Advanced Analytical Skills Training”, and “Fundamentals in Criminal Intelligence Unit Supervision/Management”. Visit the LEIU webpage at [www.leiu.org](http://www.leiu.org) for specific dates and location.
APPENDIX D

BASIC ELEMENTS OF A NETWORKING/TASK FORCE MUTUAL AID AGREEMENT

1. **Network Membership**
   - List of Participating Agencies

2. **Statement of Problem**
   - Criminal Intelligence Problem
   - Need for Combining Resources
   - Jurisdiction Statement and Reciprocity of Powers

3. **Project Description**
   - Proposal
   - Staffing Requirements
   - Contemplated Tasks
   - Duration of Agreement

4. **Structure and Organization**
   - Board of Directors
   - Management and Supervision
   - Specialized Assignments
   - Legal Assistance
   - Guidelines of Network Organization and Central Files
   - Target Selection
   - Withdrawal Procedures

5. **Personnel, Budget, and Equipment**
   - Salary and Benefits
   - Prorated costs for each agency
   - Vehicles and Special Equipment
   - Liability

6. **Goals and Objectives**

7. **Signatures of Chief Executive Officers**
APPENDIX E

CRIMINAL INTELLIGENCE ORGANIZATIONS
AND RESOURCES

Association of Law Enforcement Intelligence Units (LEIU)
www.leiu.org

On March 29, 1956, representatives of 26 law enforcement agencies met in San Francisco, California, to design a network for the coordinated exchange of criminal information between local U.S. law enforcement agencies on traveling criminals. From that date and for the next 55 years, LEIU's focus remained basically the same. However, in 2006, the mission was revised to reflect its changing emphasis on leadership. The Mission now is “to provide leadership and promote the professional management and development of the criminal intelligence function to protect public safety, privacy, and constitutional rights.”

Membership Benefits

- Access to the most up-to-date, professional and nationally-recommended standards and guidelines for criminal intelligence units
- Membership in LEIU’s established network – the oldest network – of law enforcement members committed to professional criminal intelligence practices
- A roster with around-the-clock contact numbers for designated LEIU criminal intelligence officers/analysts in approximately 200 LEIU member agencies
- Top-quality LEIU training events and seminars focusing on criminal intelligence issues
- Authoritative publications on criminal intelligence
- An independent voice in information sharing and criminal intelligence issues at the national level
- Access to LEIU’s online gaming index
- “The Source” – LEIU’s weekly briefing delivered each Wednesday on organized crime, terrorism, gaming issues and legal news.
LEIU is an agency-based membership organization of law enforcement/government regulatory agencies with approximately 200 members representing 80% of the major agencies in the U.S. and Canada.

California DOJ/BI
LEIU/Central Coordinating Agency
1825 Bell Street, Suite 205
Sacramento, CA 95825
(916) 263-1187

El Paso Intelligence Center (EPIC)
www.dea.gov/el-paso-intelligence-center-epic

Located in El Paso, Texas, EPIC supports United States law enforcement through the timely analysis and dissemination of intelligence on threats to the Nation and those criminal organizations responsible for illegal activities within the Western Hemisphere, having an emphasis on the Southwest border.

High Intensity Drug Trafficking Areas (HIDTA)
www.dea.gov/high-intensity-drug-trafficking-areas-hidta

The HIDTA program, created by Congress with the Anti-Drug Abuse Act of 1998, provides assistance to federal, state, local and tribal law enforcement agencies operating in areas determined to be critical drug-trafficking regions of the United States. There are currently 28 HIDTA’s located in 49 states, Puerto Rico, the Virgin Islands and the District of Columbia.

Homeland Security Information Network (HSIN)
www.dhs.gov/homeland-security-information-network-hsin

The Homeland Security Information Network (HSIN) is the trusted network for homeland security mission operations to share Sensitive But Unclassified (SBU) information. Federal, State, Local, Territorial, Tribal, International and Private Sector homeland security partners use HSIN to manage operations, analyze data, send alerts and notices, and in general, share the information they need to do their jobs.
The International Association of Crime Analysts (IACA) helps crime analysts around the world improve their skills and make valuable contacts to help law enforcement agencies make the best use of crime analysis and to advocate for standards of performance and technique within the profession itself. Members include crime analysts, intelligence analysts, police officers, educators and students from over 30 countries.

IALEIA is the largest professional organization in the world representing law enforcement analysts. Its purpose is to advance high standards of professionalism in law enforcement intelligence analysis at the local, state/provincial, national and international levels. It aims to enhance understanding of the role of intelligence analysis, encourage the recognition of intelligence analysis as a professional endeavor, develop international qualification and competency standards, reinforce professional concepts, devise training standards and curricula, furnish advisory and related services on intelligence analysis matters, conduct analytic-related research studies and provide the ability to disseminate information regarding analytical techniques and methods.

Interpol was founded in 1923 for the purpose of promoting mutual assistance among international law enforcement authorities, coordinating and aiding international arrests and extraditions, and providing a way to expedite the exchange of criminal justice information.
**Joint Counterterrorism Assessment Team (JCAT)**

[www.nctc.gov/jcat](http://www.nctc.gov/jcat)

The Joint Counterterrorism Assessment Team works to improve information sharing and enhance public safety. In coordination with the FBI and DHS, JCAT collaborates with other members of the Intelligence Community to research, produce, and disseminate counterterrorism intelligence products for federal, state, local, tribal agencies and the private sector. Their products include an **Intelligence Guide for First Responders** and a **Counter Terrorism Guide**.

**Joint Terrorism Task Forces (JTTF)**


The JTTF is comprised of locally based investigators, analysts, linguists and other specialists from various law enforcement agencies. It is led by the FBI and serves as the “front line” on terrorism cases by investigating leads, gathering evidence and making arrests. It also provides security for special events, conducts training, collects and shares intelligence and responds to threats.

**National Criminal Intelligence Resource Center**

[www.ncirc.gov](http://www.ncirc.gov)

The National Criminal Intelligence Resource Center manages a website, sponsored by the U.S. Department of Justice, Bureau of Justice Assistance (BJA) that provides criminal justice professionals with a multitude of resources that are primarily concerned with law enforcement intelligence operations and practices.

**National Network of Fusion Centers**

[www.nfcausa.org](http://www.nfcausa.org)

State and major urban area fusion centers serve as primary focal points within the state and local environment for the receipt, analysis, gathering and sharing of threat-related information among federal, state, local, tribal and territorial partners. They are uniquely situated to empower front-line law enforcement, public safety, fire service, emergency response, public
health, critical infrastructure protection and private sector security personnel to lawfully gather and share threat-related information. They provide interdisciplinary expertise and situational awareness to inform decision-making at all levels of government. Fusion centers are owned and operated by state and local entities with support from federal partners.

---

**Regional Information Sharing System (RISS)**

[www.riss.net](http://www.riss.net)

The RISS projects were first funded in the late 1970s, and since 1980, the U.S. Congress has made funds available from the Department of Justice budget. RISS is made up of six regional projects and the RISS Technology Support Center. Each regional project is devoted to information sharing among local and state agencies and most provide training, charting and crime expertise when requested by individual intelligence units.

The RISS Centers provide analytical services, equipment loans, investigative support, training and publications. Additionally, the centers offer a secure intranet, an integrated criminal intelligence database, and an event de-confliction capability designed to enhance officer safety.

The regional RISS Projects are:

- **Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network (MAGLOCLEN)**  
  [info@magloclen.riss.net](mailto:info@magloclen.riss.net)

- **Mid-States Organized Crime Information Network (MOCIC)**  
  [info@mocic.riss.net](mailto:info@mocic.riss.net)

- **New England State Police Information Network (NESPIN)**  
  [info@nespin.riss.net](mailto:info@nespin.riss.net)

- **Rocky Mountain Information Network (RMIN)**  
  [info@rmin.riss.net](mailto:info@rmin.riss.net)

- **Regional Organized Crime Information Center (ROCIC)**  
  [info@roacic.riss.net](mailto:info@roacic.riss.net)

- **Western States Information Network (WSIN)**  
  [info@wsin.riss.net](mailto:info@wsin.riss.net)
Harris, Don R., *Basic Elements of Intelligence*, LEAA, 1976


