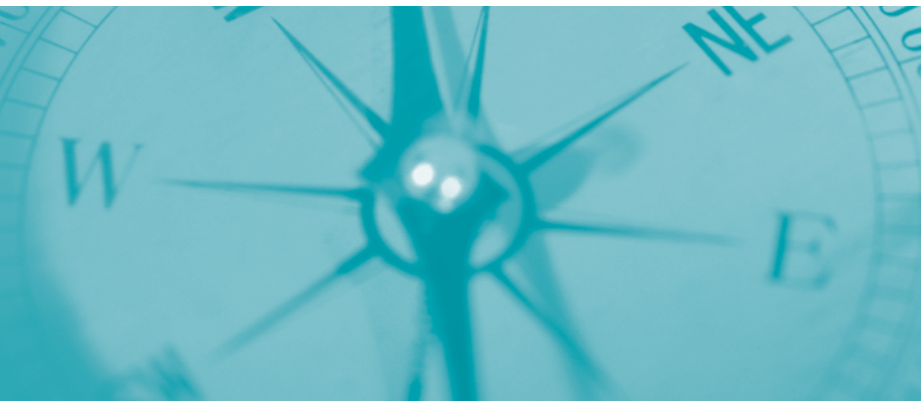


Understanding Contemporary Law
Enforcement Intelligence:
Concept and Definition



2

CHAPTER TWO

Understanding Contemporary Law Enforcement Intelligence: Concept and Definition

In the purest sense, intelligence is the product of an analytic process that evaluates information collected from diverse sources, integrates the relevant information into a cohesive package, and produces a conclusion or estimate about a criminal phenomenon by using the scientific approach to problem solving (i.e., analysis). Intelligence, therefore, is a synergistic product intended to provide meaningful and trustworthy direction to law enforcement decision makers about complex criminality, criminal enterprises, criminal extremists, and terrorists.

There are essentially two broad purposes for an intelligence function within a law enforcement agency:

Prevention. Includes gaining or developing information related to threats of terrorism or crime and using this information to apprehend offenders, harden targets, and use strategies that will eliminate or mitigate the threat. This is known as tactical intelligence.

Planning and Resource Allocation. The intelligence function provides information to decision makers about the changing nature of threats, the characteristics and methodologies of threats, and emerging threat idiosyncrasies for the purpose of developing response strategies and reallocating resources, as necessary, to accomplish effective prevention. This is known as strategic intelligence.

While investigation¹ is clearly part of the information collection² process, the intelligence function is often more exploratory and more broadly focused than a criminal investigation, per se. For example, a law enforcement agency may have a reasonable suspicion to believe that a person or group of people have the intent, capacity, and resolve to commit a crime or terrorist act. Evidence, however, may fall short of the probable cause standard, even for an arrest of criminal attempt or conspiracy. Moreover, there may be a compelling community safety reason to keep an enquiry open to identify other criminal offenders – notably leaders – and weapons that may be used.

Because of this broader role, the need to keep information secure and the necessity of keeping records on individuals for whom evidence of criminal involvement is uncertain or tangential,³ rigid guidelines must be followed. These guidelines are designed to protect the constitutional rights of citizens while at the same time permitting law enforcement agencies to proceed with an inquiry for purposes of community safety. The guidelines are also designed to facilitate accurate and secure information sharing between law enforcement agencies because the nature of terrorism and criminal enterprise threats are inherently multijurisdictional. Further, if law enforcement agencies at all strata of government subscribe to the same guidelines, information sharing can be more widespread because there is surety that regardless of with whom the information is shared, the security and integrity of the records will remain intact.

1 "Investigation" is defined as the pursuit of information based on leads and evidence associated with a particularly defined criminal act to identify and apprehend criminal offenders for prosecution in a criminal trial.

2 "Information collection" in the context of law enforcement intelligence is the capture of information based on a reasonable suspicion of criminal involvement for use in developing criminal cases, identifying crime trends, and protecting the community by means of intervention, apprehension, and/or target hardening.

3 This includes information that would be in the intelligence "Temporary File" as well as "Non-Criminal Identifying Information" as defined in 28 CFR Part 23.

Defining Intelligence

Definitions become problematic because of context, tradition, and the different use of language by specialists, generalists, and lay persons. This guide uses definitions based on generally accepted practice and standards by the law enforcement intelligence community at the local, state, and tribal levels. This does not mean that other definitions of terms are wrong, but provides a common understanding of words and concepts as most applicable to the targeted audience of this guide.

Before defining intelligence, it is essential to understand the meaning of "information" in the context of this process. Information may be defined as "pieces of raw, unanalyzed data that identifies persons, evidence, events, or illustrates processes that indicate the incidence of a criminal event or witnesses or evidence of a criminal event."⁴ As will be seen, information is collected as the currency that produces intelligence.

The phrase "law enforcement intelligence," used synonymously with "criminal intelligence," is frequently found in conjunction with discussions of the police role in homeland security. In most cases, the term is used improperly. Too often, intelligence is erroneously viewed as pieces of information about people, places, or events that can be used to provide insight about criminality or crime threats. It is further complicated by the failure to distinguish between law enforcement intelligence and national security intelligence.

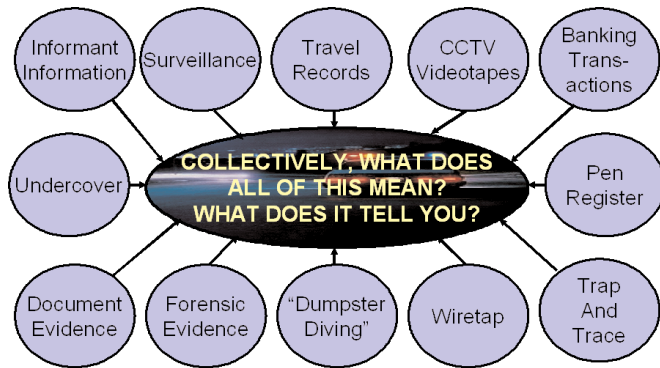
4 Global Intelligence Working Group. (2004). *Criminal Intelligence for the Chief Executive: A Training Program for the Chief Executive*. Glossary.

Law enforcement intelligence, therefore, is the PRODUCT of an analytic process that provides an INTEGRATED PERSPECTIVE to disparate information about crime, crime trends, crime and security threats, and conditions associated with criminality."⁵

Pieces of information gathered from diverse sources, for example, wiretaps, informants, banking records, or surveillance (see Figure 1-1), are simply raw data which frequently have limited inherent meaning. Intelligence is when a wide array of raw information is assessed for validity

and reliability, reviewed for materiality to the issues at question, and given meaning through the application of inductive or deductive logic. Law enforcement intelligence, therefore, is the product of an analytic process that provides an integrated perspective to disparate information about crime, crime trends, crime and security threats, and conditions associated with criminality.”⁵ The need for carefully analyzed, reliable information is essential because both policy and operational decisions are made using intelligence; therefore, a vigilant process must be in place to ensure that decisions are made on objective, informed criteria, rather than on presumed criteria.

Figure 1-1: Diverse Information Collected for Intelligence Analysis



5 Carter, David L. (2002). *Law Enforcement Intelligence Operations*. 8th ed. Tallahassee, FL: SMC Sciences, Inc.

Often “information sharing” and “intelligence sharing” are used interchangeably by persons who do not understand the subtleties, yet importance, of the distinction. In the strictest sense, care should be taken to use terms appropriately because, as will be seen in later discussions, there are different regulatory and legal implications for “intelligence” than for “information” (see Figure 1-2). As such, the subtleties of language can become an important factor should the management of a law enforcement agency’s intelligence records come under scrutiny.

Figure 1-2: Comparative Illustrations of Information and Intelligence

Information	Intelligence
<ul style="list-style-type: none"> • Criminal history and driving records • Offense reporting records • Statements by informants, witnesses, and suspects • Registration information for motor vehicles, watercraft, and aircraft • Licensing details about vehicle operators and professional licenses of all forms • Observations of behaviors and incidents by investigators, surveillance teams, or citizens • Details about banking, investments, credit reports, and other financial matters • Descriptions of travel including the traveler(s) names, itinerary, methods of travel, date, time, locations, etc. 	<ul style="list-style-type: none"> • A report by an analyst that draws conclusions about a person's criminal liability based on an integrated analysis of diverse information collected by investigators and/or researchers • An analysis of crime or terrorism trends with conclusions drawn about characteristics of offenders, probable future crime, and optional methods for preventing future crime/terrorism • A forecast drawn about potential victimization of crime or terrorism based on an assessment of limited information when an analysts uses past experience as context for the conclusion • An estimate of a person's income from a criminal enterprise based on a market and trafficking analysis of illegal commodities

Definitions and Context

State and local law enforcement have consistently defined law enforcement intelligence as containing the critical element of “analysis” before any information can be characterized as “intelligence.” For example, the Intelligence-Led Policing report funded by the Office of Community Oriented Policing Services observes that:

...intelligence is the combination of credible information with quality analysis—information that has been evaluated and from which conclusions have been drawn.⁶

Similarly, the Global Intelligence Working Group, a project funded by the Office of Justice Programs and is part of the Global Information Sharing Initiative, discusses law enforcement intelligence by observing:

...the collection and analysis of information to produce an intelligence end product designed to inform law enforcement decision making at both the tactical and strategic levels.⁷

6 International Association of Chiefs of Police. (2002). *Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing at the Federal, State, and Local Levels*. A summit report. Alexandria, VA: IACP., p. v.

7 Global Intelligence Working Group. (2003). *National Criminal Intelligence Sharing Plan*. Washington, DC: Office of Justice Programs, p. 6.

Following a consistent vision, the International Association of Law Enforcement Intelligence Analysts (IALEIA) states that intelligence is an analytic process:

...deriving meaning from fact. It is taking information collected in the course of an investigation, or from internal or external files, and arriving at something more than was evident before. This could be leads in a case, a more accurate view of a crime problem, a forecast of future crime levels, a hypothesis of who may have committed a crime or a strategy to prevent crime.⁸

Beyond these descriptions, the Office of Domestic Preparedness⁹ of the Department of Homeland Security simply defines law enforcement intelligence as:

...the product of adding value to information and data through analysis.¹⁰

In creating standards for state, local, and tribal law enforcement, the Commission on Accreditation of Law Enforcement Agencies (CALEA) seeks to provide specific guidance on policies and practices that ensures efficacy and protection from liability on all aspects of law enforcement duties. With respect to intelligence, CALEA's standards note:

Certain essential activities should be accomplished by an intelligence function, to include a procedure that permits the continuous flow of raw data into a central point from all sources; a secure records system in which evaluated data are properly cross-referenced to reflect relationships and to ensure complete and rapid retrieval; a system of analysis capable of developing intelligence from both the records system and other data sources; and a system for dissemination of information to appropriate components.¹¹

It is clear not only from these discussions, but also from the legacy of law enforcement intelligence of various national commissions examining intelligence activities at the state and local level, that a common thread is that information must be analyzed before it is classified as intelligence.”

8 International Association of Law Enforcement Intelligence Analysts. (undated). *Successful Law Enforcement Using Analytic Methods*. Internet-published document. p. 2.

9 The Office of Domestic Preparedness is not the Office of State and Local Government Coordination and Preparedness.

10 Office of Domestic Preparedness. (2003). *The Office of Domestic Preparedness Guidelines for Homeland Security*. Washington, DC: U.S. Department of Homeland Security. p.27.

11 Commission on Accreditation of Law Enforcement Agencies. (2002). *Standards for Law Enforcement Accreditation*. "Standard 51.1.1 - Criminal Intelligence." Washington, DC: CALEA.

Chapter 3 will show that there is a fundamental reason for this: regulations applying to state, local, and tribal intelligence records¹² must meet standards of assessment that do not apply to federal agencies.¹³ As a consequence, the analytic component is essential for the definition.

It is often stated that for every rule there is an exception. The definition of law enforcement intelligence fits this axiom. As a matter of functional practicality, the FBI Office of Intelligence (OI) categorizes intelligence somewhat differently. As observed by FBI Deputy Assistant Director of the Office of Intelligence Robert Casey:

In the law enforcement/national security business, [intelligence] is information about those who would do us harm in the form of terrorist acts or other crimes, be they property crimes or violent crimes. ... [The FBI OI] produces both "raw" (or un-evaluated intelligence) and "finished" intelligence products (those that report intelligence that has had some degree of analysis).¹⁴

Given the nature of the FBI OI's responsibilities and the need to get the critical threat information into the hands of the law enforcement community quickly, this definition is more appropriate for its role. Law enforcement executives need to be aware of the different roles and the different context when interpreting information. These differences are not in conflict, rather they exist to support the different missions and responsibilities of agencies at all levels of government. Similarly, the need for a different approach to the "intelligence cycle" exists more for the FBI than for state, local, and tribal law enforcement (SLTLE) because of different intelligence demands (described in Chapter 5).

12 Most notably, 28 CFR Part 23 as well as various court decisions.

13 These issues are described in detail, both in Chapter 3 and Chapter 7.

14 Robert Casey, Deputy Assistant Director, FBI Office of Intelligence. Personal correspondence July 17, 2004.

...a COMMON THREAD is that analysis must be performed on information before it is CLASSIFIED AS "INTELLIGENCE."

The remedy is simple: Those responsible for the intelligence function need to understand the differences and apply policies and practices (described later) that are most appropriate for the types of intelligence being produced and consumed.

National Security Intelligence

In understanding the broad arena of intelligence, some perspective of national security intelligence (NSI) is useful for SLTLE agencies. This primer is meant to familiarize the law enforcement reader with basic terms, concepts, and issues, and is not an exhaustive description.

NSI may be defined as “the collection and analysis of information concerned with the relationship and homeostasis of the United States with foreign powers, organizations, and persons with regard to political and economic factors as well as the maintenance of the United States' sovereign principles.”¹⁵ NSI seeks to maintain the United States as a free, capitalist republic with its laws and constitutional foundation intact and identify and neutralize threats or actions which undermine the American way of life.

15 Carter, David L. (2002). *Law Enforcement Intelligence Operations*. 8th ed. Tallahassee, FL: SMC Sciences, Inc.

16 See also www.odci.gov

NSI embodies both policy intelligence and military intelligence. Policy intelligence is concerned with threatening actions and activities of entities hostile to the U.S., while military intelligence focuses on hostile entities, weapons systems, warfare capabilities, and order of battle. Since the fall of the Soviet Union and the rise of threats from terrorist groups, both policy and military intelligence have evolved to grapple with the character of new threats. The organizations responsible for NSI are collectively known as the Intelligence Community (IC) (see Figure 1-3).¹⁶

As seen in the definition and descriptions of NSI, there is no jurisdictional concern for crime. As a result, constitutional restrictions that attach to criminal cases that law enforcement faces on information collection, records retention, and use of information in a raw capacity do not apply to IC responsibilities where there is no criminal investigation.

Figure 1-3: Intelligence Community¹⁷

An Intelligence Community (IC) member is a federal government agency, service, bureau, or other organization within the executive branch that plays a role in the business of national intelligence

- Air Force Intelligence
- Army Intelligence
- Central Intelligence Agency
- Coast Guard Intelligence
- Defense Intelligence Agency
- Department of Energy
- Department of Homeland Security
- Department of State
- Department of Treasury
- Federal Bureau of Investigation
- Marine Corps Intelligence
- National Geospatial-Intelligence Agency
- National Reconnaissance Office
- National Security Agency
- Navy Intelligence



SLTLE agencies have no direct jurisdiction as related to NSI; however, this does not mean that they will not encounter NSI nor receive collection tasks to support NSI. Indeed, given that the FBI is a member of the IC, there is a strong likelihood that SLTLE officers serving on a Joint Terrorism Task Force will encounter or be exposed to NSI. Similarly, officers working on an Organized Crime Drug Enforcement Task Force (OCDETF) may also encounter this intelligence. In both instances the officers typically will have Top Secret or Secret security classifications that provide additional details and background information. Nonetheless, it is a “slippery slope” for SLTLE officers to rely on this information for a criminal investigation because there is a strong likelihood that the methods of collecting the NSI would not meet constitutional muster in a criminal trial. Even if it appeared that constitutional standards may be met, there are other potential problems of using the information in a criminal enquiry. Since the accused in a criminal proceeding has the right to be confronted by his or her accusers, the exercise of this right could compromise sensitive sources and methods. While the Classified Information Procedures Act (CIPA) provides a mechanism to deal with the process, some find that it is cumbersome and may result in greater complications than would otherwise be necessary.¹⁸

The next issue deals with constitutional law. If the information was collected via NSI sources in a manner inconsistent with the Constitution, it is likely, based on the “Fruits of the Poisonous Tree Doctrine,” that any subsequent evidence developed during the course of that investigation

17 On August 28, 2004 President Bush announced: “I have ordered the Director of Central Intelligence to perform the functions of the National Intelligence Director within the constraints of existing law, until Congress establishes that position. I agree with the 9/11 Commission that America needs a single official to coordinate the foreign and domestic activities of the intelligence community with authority over personnel budgeting and policy. I am working with members of Congress to create this position. And while we act, the Director of Central Intelligence will play an expanded role.” www.whitehouse.gov/news/releases/2004/08/20040828.html

18 The author has elected not to discuss CIPA in any detail because it deals with federal investigations rather than state, local, and tribal criminal investigations. For the person interested in further exploring CIPA, see www.usdoj.gov/usao/eousa/foi_a_reading_room/usam/title9/crm02054.htm.

would be subject to the Exclusionary Rule. Consequently, the evidence would be inadmissible.

A final issue with respect to state, local, and tribal officers' access to NSI is liability. Specifically, if in a criminal investigation SLTLE officers used NSI that was collected in a manner inconsistent with constitutional standards or if that information (including personal records) was kept as intelligence records that were under the custodianship of a state, local, or tribal law enforcement officer, it is possible that the officer(s) and the chain of command (through vicarious liability) of that officer's agency could be liable under 42 USC 1983, *Civil Action for Deprivation of Civil Rights*. As most officers are well aware, under this provision if a state or local officer, acting under the color of state law, violates the civil rights of a person, the officer and his or her chain of command may be sued in federal court. Even though that officer may be working on a federal task force under the supervision of a federal officer such as an FBI agent, the applicable test is whether the officer is paid by and bound by the employment rules of his or her state or local employing jurisdiction.¹⁹

19 The FBI may keep such records in its custody on the basis of its national security responsibilities. While it is possible to hold a federal officer liable based on what is known as a “*Bivens Suit*” - derived from the case of *Bivens v. Six Unknown Agents* 403 US 388 (1971) – it would be difficult, particularly under the conditions of counterterrorism.

20 The Coast Guard of the Department of Homeland Security is the only other IC member authorized to collect intelligence in U.S. territory.

In sum, based on authorities from the National Security Act of 1947, Executive Order 12333, various Directives from the Director of Central Intelligence, and the U.S. Attorney General Guidelines, the FBI is the lead agency in domestic intelligence collection. It is important that SLTLE understand the distinction between the FBI's authority to both collect and produce intelligence within the territory of the United States and the authority of the Central Intelligence Agency (CIA), National Security Agency (NSA), and other intelligence community members to collect in foreign territories.²⁰ The Department of Homeland Security can produce intelligence as a result of analysis for dissemination to SLTLE. U.S. foreign intelligence agencies, however, are prohibited from working with state and local law enforcement in a manner that could be interpreted as “tasking intelligence collection.” As a result, SLTLE should rely on their relationship with the FBI in matters of intelligence collection in the territory of the U.S., including where those matters involve international terrorism activity.

The lessons learned from this brief review of national security intelligence are threefold:

1. State, local, and tribal law enforcement officers have no jurisdiction to collect or manage national security intelligence.
2. Use of NSI in a criminal investigation by a state, local, or tribal law enforcement officer could derail the prosecution of a case because of Fourth Amendment protections afforded by the Fruits of the Poisonous Tree Doctrine and the Exclusionary Rule.
3. Use of NSI in a criminal investigation by an SLTLE officer and/or retention of NSI in a records system or in the personal records of an SLTLE officer could open the possibility of civil liability from a Section 1983 lawsuit.

CONCLUSION

The intent of this chapter was to give the reader insight into what intelligence is, its role, and some of the complications that emerge from using the term. Law enforcement intelligence, for example, is defined somewhat differently by the FBI than it is by SLTLE. The reason for the difference is based on the sources of information used by the FBI and the responsibility it holds for disseminating unique critical information in a timely fashion. The important point is that the consumer simply needs to know the different definitions and the different context. With this knowledge, information can be interpreted and used most effectively.

Chapter 2 also addressed the meaning of NSI and the complications it conceivably can pose for SLTLE agencies. Once again, it is important to understand the issues and parameters of each type of intelligence. The proverbial bottom line is that understanding the definitions and their application is an essential foundation for the remaining topics discussed throughout the guide.

