LAW ENFORCEMENT POLICY CENTER

Criminal Intelligence

July 2021

IACP®
International Association of Chiefs of Police

The IACP Law Enforcement Policy Center creates four types of documents: Model Policies, Considerations Documents, Concepts & Issues Papers, and Need to Know one-page summaries. Typically, for each topic, either a Model Policy or a Considerations Document is created, supplemented with a Concepts & Issues Paper. This file contains the following documents:

- ***Considerations Document****:* Offered as an alternative to the bright-line directives found in a Model Policy. Instead of providing exact policy language, the Considerations Document outlines items that agencies should address and provides options that agencies should examine when developing their own policies on the topic.
- ***Concepts & Issues Paper****:* Designed to provide context and background information to support a Model Policy or Considerations Document for a deeper understanding of the topic.

Considerations Document

Updated: July 2021

Criminal Intelligence

I. Purpose

This document is intended to provide agencies with items for consideration when developing their own policies related to criminal intelligence, to include suggested guidelines and principles for the collection, analysis, and distribution of intelligence products. The goal of this document is to provide law enforcement agencies with the framework to establish and maintain a comprehensive and sustainable criminal intelligence capability within their respective agencies while adhering to the recommended and/or existing rules and regulations relative to civil rights (in the United States, this includes 28 Code of Federal Regulations [CFR], Part 23).[1]

II. Policy

Law enforcement agencies should develop a systematic, scientific, and logical method to comprehensively process information to ensure the most accurate criminal intelligence product is produced and disseminated to the law enforcement professionals who make decisions and/or operationally respond to prevent a criminal threat from reaching fruition. Information gathering should be directed toward specific individuals or organizations where there is reasonable suspicion that said individuals or organizations may be planning or engaging in criminal activity, to gather it with due respect for the rights of those involved, and to disseminate it only to authorized individuals as defined. While criminal intelligence may be assigned to specific personnel within the agency, all members of the agency are responsible for reporting information that may help identify criminal conspirators and perpetrators.

Agencies should develop a policy statement to concisely explain to agency personnel and the public the agency's policy on criminal intelligence.

Sample: *It is the policy of this agency's intelligence function to gather information from all sources in a manner consistent with the law and with respect to the rights of individuals; to analyze that information to provide criminal intelligence on the existence, identities, and capabilities of criminal suspects and enterprises, generally; to identify trends/patterns for use by decision makers; and, in particular, to further crime prevention and enforcement objectives and priorities identified by this agency.*

[1] 28 CFR Part 23, Criminal Intelligence Systems Operating Policies, available at https://it.ojp.gov/documents/28cfr_part_23.pdf.

III. DEFINITIONS

Analysis: Activity whereby meaning (actual or suggested) is derived through organizing and systematically examining information and applying logical reasoning. This often involves resolving or separating an idea or construct into its component parts, ascertaining those parts, and tracing parts to their source to reveal the general principles behind them.[2]

Audit: A process for ensuring that files are maintained in accordance with the goals and objectives of the intelligence authority and include information that is both timely and relevant. Audits may be conducted internally and/or by an outside agency.

Criminal intelligence: Information compiled, analyzed, and/or disseminated to anticipate, prevent, or monitor criminal activity. The intent of criminal intelligence is to gather, analyze, and disseminate information about persons who are reasonably suspected of being engaged in or preparing to engage in some form of criminal activity.[3] Criminal intelligence focuses on the activities and behaviors of individuals or organized groups of individuals in order to gather evidence for prosecution.[4] Criminal intelligence focuses on the activities and behaviors of especially noteworthy offenders or organized groups of likely offenders in order to gather evidence for prosecution. Such information is usually not widely dispersed and shared only as needed.[5] Criminal intelligence systems and processes are governed in the United States by 28 CFR Part 23.

Information: Knowledge in its raw form.[6]

Intelligence: The end product of an analytic process that evaluates information collected from diverse sources; integrates the relevant information into a logical package; and produces a conclusion, estimate, or forecast about a criminal phenomenon by using the scientific approach to problem-solving (analysis). Intelligence is a synergistic product intended to provide meaningful and trustworthy actionable knowledge to law enforcement decision makers about complex criminality, criminal enterprises, criminal extremists, and terrorists.[7] Information is not intelligence until it has undergone a series of analytical processes that determine its utility for tactical or strategic law enforcement purposes. Whereas investigations focus on events that have already occurred, intelligence is anticipatory; it informs planning and decisions.

Intelligence authority: An individual or group designated with an agency's intelligence responsibilities. In some cases, the intelligence authority may be synonymous with the Intelligence Officer in Charge (OIC). In larger agencies, it may refer to a multi-person intelligence operating unit.

---

[2] Analysis can occur to either information or intelligence. United Nations (UN), Office on Drugs and Crime, *Criminal Intelligence Manual for Analysts* (2011), **https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf**.

[3] This definition precludes actions of persons that, although they may be considered troublesome, or otherwise objectionable, do not reasonably constitute a criminal threat. These persons are not legitimate subjects of criminal intelligence gathering. This definition also precludes the conduct of counterintelligence operations by state and local law enforcement agencies. These are in the domain of federal enforcement and investigative agencies. For example, state and local police should not be involved in the investigation of espionage, sedition, subversion, and related national security concerns absent involvement or suspected involvement by the same individuals or groups in other felonious acts such as murder, arson, extortion, or kidnapping. Investigation of criminal enterprises or criminal acts may, in some cases, uncover information of a national security interest. At that time, involvement of appropriate federal agencies is warranted even though the local or state law enforcement agency may conduct concurrent or cooperative investigations.

[4] Jerry H. Ratcliffe, *Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders* (Washington, DC: Police Foundation, 2007), **https://cops.usdoj.gov/RIC/Publications/cops-w0690-pub.pdf**.

[5] Ratcliffe, *Integrated Intelligence and Crime Analysis*.

[6] UN Office on Drugs and Crime, *Criminal Intelligence Manual for Analysts*.

[7] International Association of Directors of Law Enforcement Standards and Training, "Understanding Contemporary Law Enforcement Intelligence: Concept and Definition," chap. 2 in David L. Carter, ed., *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies,* 1st ed. (East Lansing, MI: Michigan State Univ., School of Criminal Justice, 2004), **https://fas.org/irp/agency/doj/lei/chap2.pdf**.

Intelligence cycle: The process by which information becomes intelligence. The intelligence cycle is completed through active collaboration and consists of six steps: planning and direction, collection, processing, analysis and production, dissemination, and reevaluation. The cycle is circular in nature, and the movement between the steps is fluid.

Purge: To dispose of or destroy criminal intelligence in such a way that it is no longer accessible.

IV. PROCEDURES

A. General Principles

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

1. The agency should clearly define the specific objectives of the intelligence operation(s).
2. The agency should designate the individual(s) responsible for oversight of the agency's criminal intelligence function, herein referred to as the Intelligence OIC.[8]
3. While criminal intelligence may be assigned to specific personnel within the agency, all members of the agency are responsible for understanding information that is of intelligence value to the agency/unit, and where and how to report such information.

B. Information Collection

Information gathering for intelligence purposes shall be premised on circumstances that provide a reasonable suspicion (as defined in 28 CFR, Part 23) that specific individuals or organizations may be planning or engaging in criminal activity. Information-gathering techniques employed shall be lawful and only so intrusive as to gather sufficient information to prevent criminal conduct or the planning of criminal conduct.

1. Information gathering for intelligence purposes shall be premised on circumstances that provide a reasonable suspicion that specific individuals or organizations may be planning or engaging in criminal activity.
2. The Intelligence OIC (or designee) shall ensure that information added to criminal intelligence files is relevant to a current or ongoing intelligence purpose and has been verified to be the product of dependable and trustworthy sources of information. A record should be kept of the source of all information received and maintained by the Intelligence OIC (or designee).
3. The Intelligence OIC will be responsible for ensuring there is legal justification and sufficient information to conduct operations. This includes but is not limited to the following types of information:
    a. Subject, victim(s), and complainant, as appropriate; summary of suspected criminal activity;
    b. Anticipated information-gathering steps to include proposed use of informants,[9] photographs, or surveillance;
    c. Anticipated results; and
    d. Problems, restraints, or conflicts of interest.

[8] Although specific organization will vary by agency, the criminal intelligence function is typically kept separate from criminal analysis.
[9] For more information, see the IACP Policy Center resources on Confidential Informants at **https://www.theiacp.org/resources/policy-center-resource/confidential-informants**.

4. Officers shall not retain official intelligence documentation for personal use or other purposes and should submit such reports and information directly to the Intelligence OIC or designated point of contact.

C. Secure Storage

Accurate documentation and control of information and intelligence is of paramount importance. All information and intelligence files should be maintained in accordance with applicable law. Agency policy should also include the following elements:

1. **Confidentiality** – Criminal intelligence products should be maintained in confidence and marked in accordance with agency classification policy. No access should be given to another agency except with the consent of the originating agency.
2. **Classification** – Information collected will be classified in order to protect sources, investigations, and individuals' rights to privacy, as well as to provide a structure that will enable the agency to control access to intelligence. These classifications should be reevaluated whenever new information is added to an existing intelligence file.
3. **Access** – All restricted and confidential files should be stored in a secured manner (in the United States, in accordance with 28 CFR Part 23), and access to all intelligence information should be controlled and recorded by procedures established by the Intelligence OIC (or designee).
4. **Release** – All files released under disclosure requests[10] should be carefully reviewed and may be redacted, as applicable. Release of intelligence information, in general, and electronic surveillance information and photographic intelligence, in particular, to any authorized law enforcement agency should be made only with the express approval of the Intelligence OIC (or designee) and with the stipulation that such intelligence will not be duplicated or otherwise disseminated without the approval of the agency's Intelligence OIC (or designee). Intelligence products that are based on or use federal or other agency information must be reviewed by the originating agency before any Freedom of Information Act (FOIA) releases.
5. **Ownership** – Released material will remain the property of the originating agency but may be retained by another agency.
6. **Records Management** – Agencies should determine what records will be maintained. In the United States, this should include adherence to 28 CFR Part 23.[11]

D. Evaluation & Analysis

Agencies should determine the pre-assessment steps to be taken upon receipt of information in any form. These may include:

1. Evaluating and documenting the source of the information with respect to reliability and validity. While evaluation may be imprecise, this assessment should be conducted to the degree possible in order to guide others in using the information.
2. Corroborating and verifying the information using multiple independent sources.

Agencies should provide guidance regarding analysis of criminal intelligence. This process should clearly articulate who is responsible and authorized to conduct the analysis and the procedures to be followed. Where possible, the process should be accomplished by professional, trained analysts. Analytic material should be compiled

[10] This includes Freedom of Information Act (FOIA) requests in the United States.

[11] In the United States, adherence to 28 CFR, Part 23 is required if the agency's data system is funded by federal sources.

and provided to authorized sources as soon as possible where meaningful trends, patterns, methods, characteristics, or intentions of criminal enterprises or figures emerge.

Criminal intelligence is a continuous, iterative process. As new information presents itself over time, it should be incorporated into and analyzed against existing information. The utility of the intelligence file should be regularly audited; intelligence should lead to actionable directives, or the intelligence operation should be suspended. This methodology is applicable to all criminal activity. It should be continuous and ongoing with constant analysis and reevaluation.

E. Controlled Dissemination

Information gathered and maintained by the agency for intelligence purposes may be disseminated only to appropriate persons for legitimate law enforcement purposes in accordance with law and procedures established by this agency. Criminal intelligence products should be clearly marked based on their level of sensitivity in accordance with agency classification policy.

1. The agency will establish procedures for sharing information resulting from the application of intelligence (e.g., alerts, warnings, new methods/techniques being used by bombmakers) with internal and external law enforcement partners. This may include specific directives pertaining to:
    a. The purposes for sharing the information.
    b. Who is authorized to have the information.
    c. How long the information will be available.
    d. The appropriate point of contact for questions about the information.
    e. Direction for labeling and storing the information.
2. A record should be kept regarding the dissemination of all such information to persons within this or another law enforcement agency. Consider also including a record of the results of disseminated intelligence (such as arrests, seizures, etc.).
3. The criminal intelligence product will be written for maximum utility to ensure intelligence is relevant to the consumer (decision makers/law enforcement officers).
4. Reports and other intelligence material and information received by this agency may remain the property of the originating agency, but may also be retained by this agency. Such material and information should be maintained in confidence, and no access should be given to another agency except with the consent of the originating agency.

F. Periodic Review Process

The Intelligence OIC (or designee) is responsible for ensuring that files are maintained in accordance with the goals and objectives of the intelligence authority and include information that is both timely and relevant. To that end, all intelligence files should be audited on a regular basis. This may be accomplished using an independent auditor.

G. Purging Information

When a file has no further informational value and/or no longer meets the criteria of any applicable law, it will be destroyed pursuant to the relevant retention policy. A record of purged files should be maintained by the Intelligence OIC or designee.

Every effort has been made by the IACP Law Enforcement Policy Center staff and advisory board to ensure that this document incorporates the most current information and contemporary professional judgment on this issue. However, law enforcement administrators should be cautioned that no model policy can meet all the needs of any given law enforcement agency. In addition, the formulation of specific agency policies must take into account local political and community perspectives and customs, prerogatives, and demands; often divergent law enforcement strategies and philosophies; and the impact of varied agency resource capabilities, among other factors. Readers outside of the United States should note that, while this document promotes procedures reflective of a democratic society, its legal basis follows United States Supreme Court rulings and other federal laws and statutes. Law enforcement administrators should be cautioned that each law enforcement agency operates in a unique environment of court rulings, state laws, local ordinances, regulations, judicial and administrative decisions, and collective bargaining agreements that must be considered and should therefore consult their agency's legal advisor before implementing any policy.

Concepts & Issues Paper

Updated: July 2021

Criminal Intelligence

I. Introduction

This document was designed to accompany the Criminal Intelligence Considerations document established by the IACP Law Enforcement Policy Center. This paper provides essential background material and supporting information to provide greater understanding of the developmental philosophy and implementation requirements as stated in the Considerations document. It is anticipated that this material will be of value to police agencies in their efforts to establish and maintain comprehensive and sustainable criminal intelligence strategies and capabilities within their respective agencies while adhering to the recommended and/or existing rules and regulations relative to civil liberties (in the United States, this includes 28 Code of Federal Regulations [CFR], Part 23[1]).

Criminal intelligence is differentiated from crime analysis, tips, and general information relevant to policing. While the information a patrol officer gathers during regular duties can sometimes be relevant to criminal intelligence, such observations or tips do not constitute intelligence on their own.[2] Criminal intelligence and criminal analysis are considered to be separate functions, and the definition of criminal analysis is provided below only to clarify this distinction.

The need for coordinated efforts among U.S. law enforcement agencies at all levels led to the creation of the *National Criminal Intelligence Sharing Plan* in 2003, updated in 2013. The *National Criminal Intelligence Sharing Plan* 2.0 recommends, "every agency, regardless of size, has a stake in the development and sharing of criminal intelligence."[3] Often, limited resources impose constraints on what an agency can do. However, law enforcement can counter these constraints with knowledge and understanding of the criminal intelligence process to maximize available resources. For example, while large agencies may have their own intelligence unit, smaller agencies, might leverage the resources of state or regional intelligence fusion centers. Whether an agency has the resources for a dedicated intelligence unit or not, it is important, nonetheless, for all agencies to understand the guidelines of gathering, using, and consuming criminal intelligence and the potential consequences if performed improperly.

II. Background

Information gathering is a fundamental duty of any police agency. Information is used to prevent crime, pursue and apprehend offenders, and obtain evidence necessary for conviction. Efforts to identify individuals and groups that may

[1] 28 CFR Part 23, Criminal Intelligence Systems Operating Policies, https://it.ojp.gov/documents/28cfr_part_23.pdf.

[2] For further discussion of the distinction between criminal intelligence and criminal analysis, see Police Foundation and the U.S. Department of Justice, Office of Community Oriented Policing Services (COPS), *Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders*, ed. Jerry H. Ratcliffe (2007), https://cops.usdoj.gov/RIC/Publications/cops-w0690-pub.pdf.

[3] U.S. Bureau of Justice Assistance, *National Criminal Intelligence Sharing Plan* (2013), v, https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/National%20Criminal%20Intelligence%20Sharing%20Plan%20version%202_0.pdf.

employ criminal means to advance their interests requires a systematic approach to information collection and analysis. Intelligence within the law enforcement context – whether of a tactical, operational, or strategic nature – refers to the collection, collation, evaluation, analysis, and dissemination of information relating to criminal or suspected criminal activities.

When thinking about criminal intelligence, failures of intelligence that led to tragedies such as the 2001 World Trade Center attacks and the 1995 Oklahoma City bombings may come to mind. As devastating as these tragedies were, many attacks of a similar or even a potentially more devastating nature have been thwarted largely through the development and use of criminal intelligence. For example, organized crime that has traditionally occupied a great deal of the focus of intelligence operations – while still a prominent threat – has experienced serious setbacks over recent years largely due to effective intelligence gathering operations and aggressive prosecution.

The collection of information for intelligence purposes has a long history. For hundreds of years, governments and their military forces have engaged in various activities to obtain intelligence about individuals and groups viewed as threatening. However, the focus of intelligence operations by federal, state, and local police agencies has evolved over the decades based on perceived needs and threats and will continue to evolve over time. For example, during Prohibition in the United States, intelligence operations concentrated on crimes directly and indirectly related to alcohol manufacturing, smuggling, and sales and alcohol's connection to organized crime. In the post-World War II era, intelligence was used to gather information on suspected Communist organizations. During the Vietnam War period, intelligence operations shifted to information gathering on political activists and dissidents, civil rights demonstrators, and antiwar protesters. Intelligence operations have long been used to aid in monitoring and building information on organized crime operations and are still widely used in this manner, although the focus has expanded to include the involvement of international conspiracies involved in drug trafficking. More recently, intelligence operations have been directed at countering the threat of international and domestic terrorist actors and organizations.

In the aftermath of the attacks on the World Trade Center and the Pentagon on September 11, 2001, along with a rise in political extremism and the ongoing threat of other types of terroristic attacks and organized crime, the need for law enforcement intelligence operations has become even more apparent. Efforts to counter future terrorist acts within U.S. borders are not limited to federal intelligence gathering and interdiction. State and local police play a large and critical role in identifying terrorists operating individually, in cells, or on behalf of a group or purpose and coordinating intelligence of suspected groups and their activities with federal enforcement agencies.

While intelligence plays a key role in law enforcement operations, history also demonstrates that it can lead to misuse of resources or abuse of power if not properly organized, focused, and directed. Particularly during times of national emergency, one must be especially vigilant to prevent aggressive enforcement and intelligence gathering from becoming intrusions upon constitutional rights. Overly aggressive intelligence gathering operations that resemble "fishing expeditions" have been employed improperly in the past to garner sensitive or confidential information about individuals for whom there is no reasonable suspicion of criminal activity. If passed on to other law enforcement agencies as intelligence, it can form the basis for abuse of civil liberties and potential civil liability. Safeguards should be built into screening, review, and management of intelligence files. However, it is also important to emphasize the indispensable role that criminal intelligence plays in support of law enforcement and the ultimate protection of society.

Along with domestic terrorism, international terrorism, and organized crime, local law enforcement agencies also are concerned with more provincial criminal matters. The input of local patrol officers often leads to intelligence that can be applied to strategic and tactical purposes. Support of the agency's intelligence function is, therefore, the responsibility of every law enforcement officer who provides necessary information to fuel the process. If raw information provides the indispensable material to fuel the intelligence function, a professionally organized system of information evaluation, collation, analysis, and dissemination is the refinement process that turns this raw information into intelligence in support of law enforcement operations.

Even the best intelligence, however valuable, does not produce decisions. Decisions on the use of law enforcement resources are made by command personnel who use intelligence constructively within the context of their professional experience. But, without good intelligence to point the way and weigh the available options, law enforcement executives are at a serious disadvantage.

A. Definitions[4]

Analysis: Activity whereby meaning is derived through organizing and systematically examining information and applying logical reasoning. This often involves resolving or separating an idea or construct into its component parts, ascertaining those parts, and tracing parts to their source to reveal the general principles behind them.[5]

Audit: A process for ensuring that files are maintained in accordance with the goals and objectives of the intelligence authority and include information that is both timely and relevant. Audits may be conducted internally and/or by an outside agency.

Crime analysis: The process of analyzing information collected about crimes and police service delivery in order to give direction for police officer deployment, resource allocation, and policing strategies as a means of maximizing crime prevention activities and the cost-effective operation of the police department. Crime analysis focuses on patterns of reported crime and disorder, and this information is often disseminated throughout the department in statistical reports.[6]

Criminal intelligence: Information compiled, analyzed, and/or disseminated to anticipate, prevent, or monitor focused criminal activity. The term intelligence, as used within this document, refers to criminal intelligence – that is, the intent of information gathering, analysis, and dissemination as discussed in this document deals with the identification of persons who are reasonably suspected of being engaged in or preparing to engage in some form of criminal activity.[7] Criminal intelligence focuses on the activities and behaviors of especially noteworthy offenders or organized groups of likely offenders in order to gather evidence for prosecution. Such information is usually not widely dispersed and shared only as needed.[8]

Deconfliction: The process of determining and designating the responsible agency when law enforcement personnel are conducting activities in proximity to one another at the same time.

---

[4] Unless otherwise specified, definitions are drawn from David L. Carter, ed., *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies,* 2nd ed. (East Lansing, MI: Michigan State Univ., School of Criminal Justice, January 2009), **https://cops.usdoj.gov/RIC/Publications/cops-p064-pub.pdf**.

[5] Analysis can occur to either information or intelligence. UN Office on Drugs and Crime, *Criminal Intelligence Manual for Analysts* (2011), **https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf**.

[6] Jerry H. Ratcliffe, *Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders* (Washington, DC: Police Foundation, 2007), **https://cops.usdoj.gov/RIC/Publications/cops-w0690-pub.pdf**. Note: Criminal analysis and criminal intelligence are considered to be separate and distinct functions, and the definition of criminal analysis is included here only to clarify that distinction.

[7] This definition precludes actions of persons that, although they may be considered troublesome, or otherwise objectionable, do not reasonably constitute a criminal threat. These persons are not legitimate subjects of criminal intelligence gathering. This definition also precludes the conduct of counterintelligence operations by state and local law enforcement agencies. These are legitimately the domain of federal enforcement and investigative agencies. For example, state and local police should not be involved in the investigation of espionage, sedition, subversion, and related national security concerns absent involvement or suspected involvement by the same individuals or groups in other felonious acts such as murder, arson, extortion, or kidnapping. Investigation of criminal enterprises or criminal acts may, in some cases, uncover information of a national security interest. At that time, involvement of appropriate federal agencies is warranted even though the local or state law enforcement agency may conduct concurrent or cooperative investigations.

[8] Ratcliffe, *Integrated Intelligence and Crime Analysis*, **https://cops.usdoj.gov/RIC/Publications/cops-w0690-pub.pdf**.

Fusion center: A collaborative, coordinated effort to share relevant information across federal, state/provincial, local, and tribal levels of government.[9]

Information: Knowledge in its raw form.[10]

Intelligence: The end product of an analytic process that evaluates information collected from diverse sources; integrates the relevant information into a logical package; and produces a conclusion, estimate, or forecast about a phenomenon by using the scientific approach to problem-solving (analysis). Intelligence is a synergistic product intended to provide meaningful and trustworthy actionable knowledge to inform law enforcement decision makers about complex criminality, criminal enterprises, criminal extremists, and terrorists.[11] Information is not intelligence until it has undergone a series of analytical processes that determine its utility for tactical or strategic law enforcement purposes. Whereas investigations focus on events that have already occurred, intelligence is anticipatory; it informs planning and decisions.

Intelligence in its useable form consists of reasoned conclusions, suppositions, and informed judgments based on a collection and analysis of reasonably reliable information. Intelligence is more than speculation but might not always constitute a certainty. In most cases, criminal intelligence consists of evaluations of a wide variety of raw pieces of information that provide the basis for informed judgments. As a combined whole, these pieces create enough information from which to draw reasonable inferences and conclusions.

Intelligence is often further classified as follows:

- *Tactical intelligence:* Intelligence about imminent or near-term threats. Tactical intelligence often pertains to a specific criminal event and can be used immediately by operational units to further a criminal investigation, plan tactical operations, and provide for officer safety.
- *Operational intelligence:* Intelligence about short- or long-term threats that is used to develop and implement preventive responses and inform daily decisions.
- *Strategic intelligence:* Intelligence concerning existing large-scale patterns or emerging trends of criminal activity designed to assist in criminal apprehension and crime control strategies for long-term goals.

Intelligence authority: An individual or group designated with an agency's intelligence responsibilities. In some cases, the intelligence authority may be synonymous with the Intelligence Officer in Charge (OIC). In larger agencies, it may refer to a multi-person intelligence operating unit.

Intelligence cycle: The process by which information becomes intelligence. The intelligence cycle is completed through active collaboration and consists of six steps: planning and direction, collection, processing, analysis and production, dissemination, and reevaluation. The cycle is circular in nature and the movement between the steps is fluid.[12]

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

---

[9] For more information, see the U.S. Department of Homeland Security (DHS), "Fusion Centers," 2019, **https://www.dhs.gov/fusion-centers**, and U.S. DHS, "National Network of Fusion Centers Fact Sheet," 2021, **https://www.dhs.gov/national-network-fusion-centers-fact-sheet#:~:text=Fusion%20centers%20conduct%20analysis%20and,responding%20to%20crime%20and%20terrorism**.

[10] UN Office on Drugs and Crime, *Criminal Intelligence Manual for Analysts* (2011), **https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf**.

[11] International Association of Directors of Law Enforcement Standards and Training, "Understanding Contemporary Law Enforcement Intelligence: Concept and Definition," *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, **https://fas.org/irp/agency/doj/lei/chap2.pdf**.

[12] FBI, "Intelligence Cycle Graphic," June 11, 2016, **https://www.fbi.gov/image-repository/intelligence-cycle-graphic.jpg/view**.

The traditional model of policing has generally been one of reaction to reported criminal events. In a solely responsive mode, law enforcement officers spend the largest percentage of their responding to calls for service rather than anticipating and intercepting criminal activity or developing the means to thwart crime or solve problems that are the seeds of crime.[13] Under this system, a great deal of time, energy, and expense has been expended in order to perfect ways in which officers could respond more quickly to such events, whether that be through computer-aided dispatch or other means. However, it wasn't until the Kansas City Preventive Patrol Experiment[14] and related research in the 1970s that the profession began to question the effectiveness of this purely responsive form of police operations.

Law enforcement intelligence operations are one important means of developing more proactive policing strategies. Intelligence that, for example, allows officers to intervene more effectively in ongoing criminal enterprises and ferret out criminal activity is simply smarter policing. But criminal intelligence gathering, if not organized properly and subjected to internal and external controls, can form an unwarranted or even illegal intrusion upon the rights of individuals. The law enforcement agency's mission, as well as the intelligence unit's policies and procedures and collection plan should reflect these concerns and controls.

Intelligence product: Report or document that contains assessments, forecasts, associations of individuals, organizations, and groups reasonably suspected of being involved in the actual or attempted planning, organizing, financing, or commissioning of criminal acts.

Terrorism: Violent, criminal acts committed by individuals and/or groups who are associated with or inspired by designated foreign terrorist organizations or nations (i.e., state-sponsored terrorism) or ideological influences (i.e., political, religious, social, radical, or environmental-natured ideology).[15]

Reasonable suspicion: Speculation of involvement in criminal activity based on observable cues and logical inference.[16] The threshold for collecting information and producing criminal intelligence in the U.S. is the "reasonable suspicion" standard, according to 28 CFR, Part 23, Section 23.3 c. According to the United Nations Office on Drugs and Crime, *"Reasonable suspicion is present when information exists which establishes sufficient facts to give…a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable terrorist or criminal activity or enterprise."*[17]

B. Legal Guidelines

When conducting criminal intelligence operations, officers and related personnel should adhere to the legal standards of intelligence operations, as well as any applicable national, state/provincial, or local laws and ordinances. In the United States, criminal intelligence activities are governed by 28 CFR, Part 23. It is the originating agency or collaboration of agencies who hold the responsibility of establishing that their information was collected without legal violations, or it is their duty to delegate this burden of proof to a properly trained participating agency.[18] Other topic areas that may have legal implications include security of information; operational security practices; storage and

[13] For a more complete understanding of problem-solving and its impact on crime prevention see Herman Goldstein, *Policing a Free Society* (Cambridge, MA: Ballinger Publishing, 1977).

[14] George L. Kelling, Anthony Pate, Duane Dieckman, Charles E. and Brown, *The Kansas City Preventive Patrol Experiment: A Technical Report* (Washington, DC: The Police Foundation, 1974).

[15] FBI. "Terrorism," June 11, 2016, **https://www.fbi.gov/investigate/terrorism**.

[16] See also Terry v. Ohio, 392 U.S. 1, 27 (1968), **https://supreme.justia.com/cases/federal/us/392/1/#27** .

[17] UN Office on Drugs and Crime, *Criminal Intelligence Manual for Analysts*, 92, **https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf**.

[18] Exec. Order No. 12291, 28 CFR Part 23, Criminal Intelligence Systems Operating Policies, **https://it.ojp.gov/documents/28cfr_part_23.pdf**.

retention of law enforcement intelligence and information; as well as privacy, civil rights, and civil liberties protections.[19]

In the United States, the Freedom of Information Act (FOIA) gives the public the right to request access to records from any public agency. Agencies must comply unless the requested information is protected by one of nine exemptions, which generally includes protecting national security, personal privacy, and law enforcement interests.[20] Although most criminal intelligence operation records may fall under the exemption protections, agencies should keep in mind that the Freedom of Information Act can still apply to their work.

C. Policy

Criminal intelligence is a crucial component in effective law enforcement operations, and creating a criminal intelligence policy is one critical aspect of an intelligence operation within a law enforcement agency. The policy should clearly define the mission, goals, and objectives of the intelligence function; acceptable procedures and limitations for collecting, analyzing/evaluating, auditing, purging, and disseminating intelligence; and accountability for these functions. Aspects of this policy should consider staffing and organizational strategies, legal guidelines, and information sharing strategies. It is important for agency personnel to understand the exact policy of the department to know what guidelines to adhere to when performing criminal intelligence functions. There are many aspects that may pertain to or fall under the umbrella of criminal intelligence, so providing guidance to officers and other pertinent staff is beneficial to the productivity of the personnel and to the goal of the department as a whole.

The policy should make clear the position that intelligence operations will be directed toward persons or organizations only when there is reasonable suspicion that they are involved in criminal activity. The means for ensuring that this mandate is followed are best addressed in the intelligence unit's procedural and management practices. Policy should also make it clear that the means used to develop such information cannot overlook the rights of individuals guaranteed under any applicable federal and state/provincial constitutions. These legal protections and individual rights cannot be placed on hold as a matter of convenience to achieve agency or intelligence objectives. The fact that officers cannot disregard their responsibility to the law or circumvent the rights of individuals as prescribed by law in the course of developing and managing intelligence information is a matter that deserves repetition and reinforcement in a policy on intelligence as well as in the agency's code of conduct and core values.

The policy should also emphasize confidentiality issues involved in disseminating intelligence. Distribution of intelligence to authorized persons and agencies is generally described in terms of those who have a need and right to know. A recipient agency or individual has a "need to know" when the requested information is pertinent to and necessary for the initiation or furtherance of a criminal apprehension. A "right to know" may be satisfied when the recipient agency or individual has the official capacity and statutory authority to receive the intelligence requested. Both of these conditions may need to be satisfied based on the nature and sensitivity of the information requested and the law surrounding the release of particular types of information or intelligence. The requirements and procedures for distribution should be specified and included.

Finally, policy should also emphasize the fact that information gathering for intelligence not only is the responsibility of those assigned to the intelligence authority but is driven largely by personnel throughout the agency who contribute information for assessment. The vast majority of information used by an intelligence authority is the product of observations made or information developed or received by patrol officers and investigators. Without their inputs, the intelligence function would be ineffective.

---

[19] Global Justice Information Sharing Initiative, *Law Enforcement Analytic Standards*, 2nd ed. (International Association of Law Enforcement Intelligence Analysts, Inc., 2012), **https://it.ojp.gov/documents/d/Law%20Enforcement%20Analytic%20Standards%2004202_combined_compliant.pdf.**

[20] U. S. Department of Justice, "What Is FOIA," **https://www.foia.gov/about.html**.

III. PROCEDURES

When compiling criminal intelligence, agencies should use the intelligence cycle/process, which includes:

1. Planning/direction
2. Collection of information
3. Processing/collation
4. Analysis
5. Dissemination
6. Evaluation and feedback[21]

A. Planning & Direction

Mission – While a policy or mission statement is meaningless without strong management oversight, it is the starting point for direction and control of a professional intelligence function. The intelligence function should be clearly focused and must subscribe to articulated goals and objectives that flow from an espoused statement of purpose. Some of the problems that have plagued police intelligence gathering operations over the years have been the result of information-gathering operations that have not been limited by reasonable boundaries or regulated by adherence to a precise mission or self-imposed set of standards. A sample mission statement might read as follows:

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

The mission statement is operationalized by what is often referred to as a "collection plan" that serves as the authority for, as well as the rules and regulations for the collection and distribution of intelligence and administrative control of unit operations. Moreover, the collection plan provides direction to the intelligence unit by defining, focusing, and prioritizing its operations in crime areas that directly affect the community. The plan should be a collaborative product of command personnel including the chief and may include the authority, rules, regulations, policies, and procedures relative to the intelligence unit.

The collection plan establishes intelligence objectives and intelligence collection targets. This plan should be the product of collaborative efforts on the part of key agency decision makers and may include the perspectives and perceived priorities of members of local or state government. The plan serves to identify and prioritize the primary criminal threats affecting the jurisdiction and the appropriate methods and necessary resources for developing requisite information to support enforcement actions and provides the authority for tasking these assignments. This document is dynamic in that targets and priorities will change over time and require periodic review of targets and the respective priorities.

A policy (as described above) serves as a companion document to the collection plan. The policy provides personnel with a clear understanding of the functions of, limitations upon, and accepted procedures for unit personnel. By specifying acceptable and unacceptable intelligence practices and procedures to be followed, there is less chance that abuses will occur.

Strategy – The intelligence function has often been misunderstood and, as a consequence, is sometimes a mismanaged function. In order to serve the true decision-making goals of an intelligence unit, its management and

[21] UN Office on Drugs and Crime, *Criminal Intelligence Manual for Analysts* (2011), 10–16, https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf.

organizational structure must, in some regard, be separated from day-to-day operational demands. This is not to say that tactical information cannot or should not be a legitimate product of intelligence units. However, officers should not be recruited for or serve in intelligence units under the guise that they are to serve as a select investigative unit. In both large and small law enforcement agencies, administrators must guard against the tendency to make the intelligence function simply an extension of criminal investigations or related operations. In smaller agencies, this ideal is more difficult to achieve given personnel and related resource limitations and the mere fact that there is often less need for and consequently fewer demands upon the intelligence function.[22]

The Officer in Charge (OIC) of the intelligence function should establish a routine reporting schedule to the office of the agency chief executive or his/her designee. Generally, such reporting should provide, among other things, information on the quantity and nature of intelligence operations and objectives being pursued by the unit, some measurement of the manpower involved and success on objectives, and a review of the nature of any problems facing the intelligence function either operationally or administratively. In addition to providing periodic reporting, the intelligence authority should have ongoing access to the chief executive to provide strategic and tactical information updates as circumstances dictate.

There is often an operational distrust of intelligence largely because it develops a separate body of knowledge within the police agency that can, and often does, lead to changes in law enforcement agency policy and policing strategy. To the degree that strategic intelligence leads to alterations in strategies that are either politically or institutionally unpopular, the intelligence function may face some degree of mistrust among officers. However, this mistrust can be overcome through development of an appreciation and understanding of the role of the intelligence function among line officers and the valuable role that it plays in identifying crime problems, developing strategies for their solution, and providing necessary tactical information to assist officers in their enforcement activities.

Staffing & Organization – The great diversity of law enforcement agencies will, by necessity, require that individual intelligence operations conform with local agency capabilities and needs. Yet, there are some general guidelines and recommendations that can be made in this regard that are relevant to most intelligence operations. In particular, the intelligence function should be under the control and management of one Intelligence OIC who oversees direction of its operations and management and administrative oversight consistent with the unit's mission and collection plan. While this individual may, in smaller agencies, also serve in related areas of the department and assume additional command responsibility, one person should assume responsibility for and command of the intelligence function.

Given the often-sensitive nature of the information collected by this operation, the Intelligence OIC should report directly to the chief executive officer of the agency.[23] In so doing, intelligence avoids potential filters through other channels and allows the chief executive additional lead time to conduct necessary planning. In addition to the sensitivity of the information involved, reporting directly to the office of the agency chief is justified by virtue of the nature of the intelligence function. That is, this organizational arrangement helps to prevent the undue involvement of intelligence unit personnel in line operations. For example, there is often a tendency for investigative officers or patrol commanders to co-opt the services of the intelligence unit to assist in criminal cases. While such assistance may be needed and ultimately authorized, it is far more difficult to maintain the focus of the intelligence function and control its work consistent with identified plans and objectives if it is organizationally or functionally integrated with investigative operations or other elements of the department. If command and control is lacking, it is common to find intelligence analysts being used as augmentations to or support personnel for criminal investigators. This not only serves to siphon off valuable time of intelligence personnel but also risks the possibility of intelligence personnel

[22] In some cases, agencies may prefer to work with multijurisdictional fusion centers to strengthen criminal intelligence capabilities.

[23] In some situations, particularly in larger agencies, the Intelligence OIC may report to a designee of the agency chief executive.

becoming involved in information-gathering operations that are inconsistent with the role, mandates, and even the legal and professional standards of the unit.

Broad exposure to law enforcement operations is an advantage for prospective intelligence officers, depending upon the scope of duties assigned to the intelligence staff member. However, it is not a requirement. Professional staff with sufficient acumen have been used to staff intelligence operations. A combination of professional staff and sworn personnel to staff the intelligence function is needed in order to attain the proper blend of knowledge, skills, and abilities. Some law enforcement agencies with sufficient demand may be fortunate enough and have adequate resources to employ professional law enforcement intelligence analysts.[24] For other agencies, staffing the intelligence function can be challenging– especially smaller agencies with limited resources or lack of demand for intelligence. Typically, personnel assignments in these departments are part-time in nature, sharing their time with related functions in crime analysis, investigations, research, and planning or related functions. However, the recommended minimum personnel assignment is regarded by some experts as one full-time position with no collateral duties.[25]

Intelligence analysts should have specialized training in such processes as link analysis, strategic analysis, financial analysis, and investigative analysis, and the use of computers to perform these functions. Intelligence analysts should also possess intellectual curiosity, tenacity, the ability to rapidly assimilate and recall information, and self-discipline. Additionally, intelligence officers should have a basic understanding and appreciation for the philosophical precepts of democracy and the need to protect individual liberties and should, as a condition of employment, agree to periodic polygraph examinations directed toward the discovery of misconduct or abuses of the law and civil liberties.[26] While the latter of these recommendations may test reasonable grounds for the position, it does emphasize the necessity to ensure that intelligence personnel have a strong understanding and appreciation for the potential abuses and liability associated with their work and the need to work within the parameters of agency policy and procedures.

B. Information Collection

Information gathering for intelligence purposes must be premised on circumstances that provide a reasonable suspicion that specific individuals or organizations may be planning or engaging in criminal activity. Procedures must be established for the opening of a criminal intelligence file (see "File Status," below). Authorization for opening such files and initiation of intelligence operations must be based on reasonable justification. Some suggested parameters of a preliminary intelligence information gathering include a national and local criminal history check, query of informants, physical surveillance, and interviews of witnesses and victims.[27]

Inappropriate intelligence operations include those that directly or indirectly gather information on persons based solely on their dissident political activities or views; because they espouse positions or philosophies that are perceived to threaten conventional social or political doctrine, traditionally accepted social mores, or similar societal values or institutions; or because they have cultural connections with terrorists. Use of law enforcement intelligence resources to intimidate, inhibit, or suppress such activities or harass such individuals under the pretext of legitimate police concern for maintaining social order are at best misguided and at worst constitute a threat to the principles of law

[24] The International Association for Law Enforcement Intelligence Analysts (IALEIA) provides certification programs in this law enforcement discipline and training is offered through a variety of state and national sources to include the state and local law enforcement training program at the Federal Law Enforcement Training Center (FLETC).

[25] *Criminal Intelligence Program for the Smaller Agency*, California Peace Officer's Association, Organized Crime Committee, October 1988.

[26] James R. Ferris, "A Model for Police Intelligence Units," in Michael J. Palmiotto ed., *Critical Issues in Criminal Investigation*, 2nd ed. (Cincinnati, OH: Anderson Publishing, 1988).

[27] Ferris, "A Model for Police Intelligence Units," 88.

enforcement in a democratic society. Additionally, misguided intelligence gathering wastes valuable resources that are desperately needed to ferret out wrongdoers and persons who pose real threats to national and local security.

Information collection techniques employed must be lawful and only so intrusive as to gather sufficient information to prevent criminal conduct or the planning of criminal conduct. This requires mature administrative control and sound judgment to implement and enforce. This is particularly the case when intelligence operations are involved in attempts to develop information on criminal actions that might occur as opposed to those that have occurred. Most intelligence operations are anticipatory in nature; by their nature, these types of intelligence operations are less focused, often employing the principle of the fishing net rather than the fishing spear.[28] By frequenting locales where known or suspected criminals hang out; by contriving a ruse to see, overhear, or otherwise gain knowledge of criminal plans and those persons involved or potentially involved in those plans; or by using other generally passive means, officers may develop sufficient information to pursue more active operations.

In such operations, the question often arises concerning the lengths to which officers should go in order to establish sufficient information to proceed with more active or aggressive intelligence information gathering. For purposes of policy, only general guidelines can be offered to frame such decisions. The experienced intelligence supervisor must make reasonable judgments based on the circumstances involved and the information available in given situations. In so doing, some perspective can be gained by attempts to weigh the intrusiveness of proposed intelligence and information-gathering measures against the degree of harm of the potential or suspected criminal actions. For example, the use of so-called "sneak and peek warrants,"[29] video surveillance, and other relatively intrusive measures would probably be difficult to justify in instances where the degree of harm of suspected criminal activity does not incorporate violence or other serious, high-profile felonies.

The methods of collecting information for use in the intelligence function as well as the means of reporting such information are purposely not incorporated in the model policy. These technical and procedural considerations (such as covert surveillance techniques and overt means of information gathering) are beyond the scope of this document but have been adequately addressed elsewhere.[30] However, intelligence collections must be conducted within the limits of the law. Failures in this area are most likely when officers are engaged in covert intelligence gathering operations.

File status – File status is an important issue that has bearing on both the manageability of information within the intelligence function as well as the protection of the rights of persons whose identities are housed within intelligence files. Intelligence files should be classified as either "open" or "closed,"[31] with open intelligence files including cases

[28] For a comprehensive treatment of the nuances and dilemmas of undercover and intelligence operations see, for example: Gary Marx, *Undercover: Police Surveillance in America*, University of California Press, 1988.

[29] The so-called "sneak and peak warrant" authorizes law enforcement officers to make a clandestine entry, examine the premises and then depart without seizing tangible evidence. They are, in effect, warrants authorizing information-gathering incursions onto a suspect's premises. While they are controversial in some jurisdictions, they have been upheld in federal courts. See, for example, the Second Circuit's ruling in *United States v. Villegas*, 899 F.2d 1324 (2nd Cir. 1990); cert. denied, 498 U.S. 991 (1990), in which the court noted, there must be a showing of reasonable necessity for delaying notice of the search and appropriate persons must be notified within a reasonable time after the entry. The federal courts have upheld both the concept of a covert entry and the seizure of intangible evidence. While such warrants are constitutionally acceptable, they must particularly describe the place to be searched to meet these requisites and failure to do so will result in the sneak and peak warrant being found to be unconstitutional.

[30] The reader may wish to explore these issues in such publications as the United Nations Office on Drugs and Crime, *Criminal Intelligence: Manual for Managers*, available at **https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Managers.pdf**, or the *National Criminal Intelligence Resource Center* at **https://www.ncirc.gov/Policies.aspx**.

[31] Some agencies employ additional classifications for their intelligence file, most notably those denoting a "pending" status. While such classifications may be used, they tend to add a layer of confusion into file management. If the use of a pending file status is deemed appropriate for an agency, steps should be taken to ensure that this status can be maintained for only a limited time period.

that are actively being worked. All agencies should define their own policies and procedures for opening, maintaining, and closing an intelligence file.

1. *Opening an intelligence file* – Many agencies limit the collection of intelligence to those criminal problems identified in the collection plan or as authorized by the agency chief executive. In addition to answering whether the information is crime-related and fits the mission of the intelligence unit, the intelligence function must identify minimal requirements for opening an intelligence file.
2. *Maintaining an intelligence file* – Open files must include status update reports on a regular basis.[32] To accomplish this, the intelligence function must maintain an index of intelligence file statuses in order to ensure that status reports are filed routinely as required.

   Many intelligence functions resemble the tendency of persons who have difficulty throwing out old possessions that have outlived their usefulness or value. The underlying motive among many intelligence officers like this is that more information is always better, and, even though it may not have immediate value, it may eventually be linked to other information that will make it worthwhile. While on occasion this may prove to be the case, it is the exception rather than the rule. More often, where files remain open without merit or appropriate justification, they become obsolete and may jeopardize the civil rights of persons for whom no rational criminal connections or involvement can be demonstrated.

   Where intelligence files remain open indefinitely or without justification and management oversight, they also become part of an ongoing work inventory that does not accurately reflect the intelligence function's caseload. They also can serve to inhibit intelligence officers from focusing on priorities and properly managing time and effort. And, like an extraneous piece of a jigsaw puzzle, obsolete files often serve no other function than to confuse the picture.
3. *Closing an intelligence file* – Closed intelligence files are those in which operations have been completed, where all logical leads have been exhausted, or where no legitimate law enforcement interest is served. All closed files should include a final case summary report.

C. Processing & Collation

Law enforcement officers should submit all intelligence-related information and file materials to the intelligence authority and must not retain official intelligence documentation for personal reference or other purposes. This requirement is designed primarily to help ensure that information submitted to the intelligence function is inclusive of all data necessary to make it useful for intelligence purposes. For example, the ability of intelligence analysts to conduct link analyses and perform other assessments of information in order to make it useful for intelligence purposes is dependent on the scope, detail, and accuracy of the raw data and information received. Use of standard reporting mechanisms, to include a supervisory review of all submissions to the intelligence function, is one means of helping to make this possible.

Raw data received by the intelligence function must meet several basic criteria. These include determining whether the information is crime-related, whether it is related to the mission of the intelligence function (e.g., is consistent with the collection plan), and whether the information has been or can be verified. Once affirmative answers have been reached for each of these inquiries, intelligence analysts must determine reliability and validity of the information. While evaluation may be imprecise, this assessment must be made to the degree possible in order to guide others in using the information. A record should be kept of the source of all information where known.

Potential intelligence material should be assessed based on the criteria of reliability and validity. Reliability refers to the degree to which one can depend upon or trust the information source. Validity relates to the accuracy of the

[32] Recurring at least every 180 days is recommended, though agency policies may vary.

information received. In many cases, these two elements are closely interrelated. For example, an eyewitness account by a seasoned professional law enforcement officer would normally lead one to assume both strong reliability and validity, but this may not always be the case, and it is a good matter of practice to evaluate each of these criteria separately. When reliability or validity are in doubt, restrictions should be placed on the dissemination and use of the information until such verification can be made.

In essence, this professional standard attempts to deal with the problem of quality control. Failure to institute standards of quality assurance can result in serious problems. For example, lack of quality control can result in the inclusion of data in intelligence files that erroneously and unjustly implicates or suggests the implication of individuals in criminal activity. Such errors may result in privacy or civil rights violations and potential civil litigation, particularly where such information is used as the basis for more intrusive or other covert intelligence operations. Inclusion of unfounded or erroneous information can also constitute a waste of valuable resources by siphoning them into areas of investigation that are groundless.

In the course of conducting intelligence information collection activities, officers invariably come upon a variety of information about target individuals, accomplices, and involved or uninvolved third parties. This ranges from information on a person's habits and tastes to items of a personal and highly sensitive nature that may not have any relevance on the potential or actual criminal culpability of the individual. Where this information is relevant to an operation, it can and should be included in intelligence files if found to be valid and reliable. However, information that has no direct bearing on furtherance of an ongoing operation should not be retained in intelligence files.

To assist in ascertaining the validity and reliability of information and maintaining accountability for these matters, police intelligence operations should maintain a record of the source of all information received and maintained by the intelligence authority. Many law enforcement agencies operate a criminal intelligence database for this purpose.

D. Analysis

Agencies should provide guidance regarding analysis of criminal intelligence.[33] This process should clearly articulate who is responsible and authorized to conduct the analysis and the procedures to be followed. The intelligence function should establish and maintain a process to ensure that information gathered is subjected to review and analysis to derive its meaning and value. Where possible, this process should be accomplished by professional, trained analysts. Analytic material (i.e., intelligence) compiled should be provided to authorized recipients as soon as possible where meaningful trends, patterns, methods, characteristics, or intentions of criminal enterprises or individuals emerge.

If resources allow and there is sufficient demand, agencies might consider investing in analytic software that enables communication with other silo databases for ease and completeness of analysis. Current software enables agencies to connect all data in one place for access and analysis. This can include agency internal databases, public records data, social media data, website content, other open-source intelligence (OSINT) sources, and any other databases where permission is given to search. This lets departments generate better results much faster by eliminating the time and risk of error associated with manually locating and preparing data for analysis.

Such software can also provide a range of advanced facilities for data access and analysis, including search, link charts, geospatial analysis, and entity extraction. A department can easily create and save their own visual queries and can easily and securely share data (see Section E, below) and results with selected colleagues using such software. Departments can accelerate their work by creating alerts in the software such that they are instantly informed when there are conditions of interest. Departments also can easily generate risk scores to prioritize what to look at. Visual

[33] In the U.S., this process should adhere to the Director of National Intelligence, Intelligence Community Directive 203: Analytic Standards, **https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf**.

queries can easily be shared, reused, and modified, and selected use of artificial intelligence capabilities can further help departments get faster results. If desired, this type of software can be used as part of an automated enterprise workflow. ***However, while software can be a useful tool to analysts, human interpretation of the software's results is crucial.***

E. Dissemination

Criminal intelligence efforts are invaluable to law enforcement, but silos of criminal intelligence data, while locally effective, can hamper critical information sharing since criminal activity is international in scope and movement. Agencies are not mandated to share information but should consider doing so in the appropriate circumstances. Information gathered and maintained by an agency for intelligence purposes may be disseminated only to those with appropriate clearance on a need-to-know basis for legitimate law enforcement purposes in accordance with law, as well as procedures established by the agency. A record should be kept regarding the dissemination of all such information to persons within this or another law enforcement agency.

Dissemination of such information should be limited only to persons with a need and a right to such information. Certainly, information should be forwarded only to authorized law enforcement personnel who can ensure that it will be used for legitimate law enforcement purposes and be subjected to at least the same level of safeguards as the sending agency. Since individual states often have specific requirements concerning the release of such information, intelligence personnel must be thoroughly familiar with any local or state statutes of relevance to this issue.

The importance of intelligence file security should be readily apparent. Concerns for the security of intelligence include matters relating to the sensitivity of both strategic and tactical information to the law enforcement agency, the identity of confidential informants and other sources of information, the identity of undercover police operatives, the nature of law enforcement tactics and strategies, the status of various sensitive criminal investigations, and protection of the rights of persons who are the subject of intelligence files, among other matters.

Intelligence files must be classified with regard to the sensitivity of information that they contain. Classification protects sources, investigations, and individuals' rights to privacy, and provides a structure that enables the agency to control access to intelligence. Any intelligence file must be clearly marked based on who should be able to access it. Agencies should follow the classification standards as applicable to their jurisdiction. For example, classifications might include designations such as "sensitive," "law enforcement sensitive," "sensitive but unclassified," "proprietary," and "for official use only." However, federal agencies typically use different classification systems than do municipal agencies. As intelligence files are modified on an ongoing basis, their security classification must be reevaluated whenever new information is added to an existing intelligence file.

Individual intelligence authorities must make policy determinations regarding the persons and organizations that are generally eligible to receive intelligence in the foregoing categories. However, individual decisions generally have to be made by the Intelligence OIC or their designee for release of particular items of intelligence. Factors that have bearing on these decisions vary but include, for example, assurance that recipients have not misrepresented themselves; that they are authorized to make the request and receive the information and have a need and a right to know; that disseminations can be made in accordance with law; that the information requested has adequate validity and reliability to be shared; and determination as to whether any conditions concerning the source of the data necessitate limiting its dissemination or adding conditions to its release.

When approval of intelligence dissemination has been granted, the outgoing material, appropriately marked with its security classification, should be accompanied by any requirements, restrictions, or instructions concerning its use or further dissemination. Before intelligence materials can leave the unit, either through internal or external means of dissemination, it must be recorded and indexed by the intelligence authority. Files released under Freedom of Information Act (FOIA) provisions or through discovery must be carefully reviewed. Information that is not specifically requested or for which the requesting party is not legally entitled under relevant state or federal FOIA

provisions may be deleted or redacted. Information that is properly requested pursuant to applicable laws and which is otherwise discoverable should be released.

Restricted and confidential files should always be maintained in a highly secure environment. Intelligence personnel should be ever mindful of the sensitivity and security of this documentation and consistently follow agency policy as well as any local and state laws regarding intelligence security. Hard copy file security should be practiced at all levels and computer access restricted through physical measures and by means of password and/or other protections. The intelligence facility should be housed in a location that can be fully secured and files secured separately within that location. Access of personnel to this location should be controlled and a record maintained of personnel when they are permitted access. Uncontrolled access to or improper security for intelligence files can have privacy rights implications for named individuals and potentially risk harm to witnesses, victims, police officers, and informants. Accordingly, informant files should be maintained separately from intelligence files just as they should from other intelligence files within the agency.[34]

To develop an audit trail, agencies must maintain a record of individuals and agencies with whom intelligence information has been shared. Information that is released widely ("pushed") is difficult to manage. However, information may be shared through established networks such as the Homeland Security Information Network (HSIN)[35] for more effective management. In these cases, users of the network have already been vetted and must actively seek out ("pull") the information being shared. It is easier to track and manage who views or downloads the information when that information is pulled than when it is pushed. In like manner, recipient agencies should always record the source of intelligence received from other agencies. This should be done so that the information may be verified, authenticated, or validated, if needed, at a later date, as well as to indicate to users within the agency that the information was not necessarily collected, screened, or evaluated in accordance with established agency policy.

In addition to the above, the issue of sharing intelligence must be subject to particular safeguards and controls given the fact that receiving agencies are reliant upon the validity and reliability of such information. Information passed on without adequate internal quality control review can be received and used as the factual basis for investigations when such conclusions are not warranted. The National Strategy for Information Sharing sets forth five principles that should govern information sharing:[36]

1. Fusion centers can be valuable to the information sharing process (further discussed below).
2. Effective information sharing stems from partnerships among federal, state/provincial, local, and tribal authorities, as well as international and private-sector partners.
3. During the sharing process, information might be uncovered during one operation that may pertain to another. Although such information might initially seem unrelated, it can be pertinent to other investigations or the operations of other agencies. Maintaining good professional partnerships with other agencies can help encourage information sharing practices and potentially help investigations/operations of partner agencies.
4. Information sharing practices should be included throughout the entire criminal intelligence process. This can include sharing information after the conclusion of an investigation or intelligence operation if it pertains to another agency's case.

[34] For information on informant management and file control see *Confidential Informants*, IACP Law Enforcement Policy Center, **https://www.theiacp.org/resources/policy-center-resource/confidential-informants**.

[35] For more information, see "Homeland Security Information Network (HSIN)," **https://www.dhs.gov/homeland-security-information-network-hsin**.

[36] David L. Carter, ed., *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, 2nd ed. (East Lansing, MI: Michigan State Univ., School of Criminal Justice, 2009), **https://cops.usdoj.gov/RIC/Publications/cops-p064-pub.pdf**.

5. The procedures, protocols, and operating systems that support the information sharing function should integrate existing technical capabilities as well as established authorities and responsibilities.

Information portals have been developed to support information sharing by many governmental entities around the world. In the U.S., for example, intelligence information may be shared through the HSIN. The Office of the Director of National Intelligence (ODNI) has also supported information sharing efforts by funding fusion centers to connect criminal intelligence databases to the Regional Information Sharing Systems (RISS) database, RISSIntel.[37] The RISS program is congressionally funded with oversight from the U.S. Department of Justice. RISS maintains a criminal intelligence application for law enforcement, allowing for a nationwide search of criminal intelligence databases. Other fusion center systems vary, and some fusion centers do not have access to certain databases pertaining to criminal records. In these cases, a Memorandum of Understanding or a Management Control Agreement may be used between the fusion center and a police agency that does have access to that information. Agencies should ensure their information sharing practices adhere to national or other applicable standards.[38]

In order to control the distribution of intelligence between police agencies, reports and other material shared across agencies should remain the property of the originating agency but may be retained by other agencies. Such material must be maintained in confidence, and no access should be given to another agency except with the consent of the originating agency. This directive is an attempt to prevent the distribution of intelligence between agencies without the knowledge and consent of the originating agency. In addition, prior to distribution, the originating agency should ensure that the recipient individual or agency has a need and a right to know such information. Intelligence should not be distributed without the approval of the Intelligence OIC or other agency-designated officer. Further, whenever intelligence reports or information is forwarded to another agency, a record of the transaction should be logged by the originating agency and the transaction predicated upon the understanding that further distribution is prohibited without the originating agency's approval. The same holds true for the internal distribution of intelligence.

F. Evaluation and Feedback[39]

Criminal intelligence is a continuous, iterative process of ongoing evaluation. As new information presents itself, over time, it should be incorporated into and analyzed against existing information. This methodology is applicable to all crimes and should be continuous and ongoing with constant analysis and reevaluation.

Feedback should be solicited from any recipients of intelligence products, and agencies should define a process for doing so. Intelligence products typically provide contact information for the user to provide feedback on its utility. As a recipient of an intelligence product, consider the ways in which the intelligence was used, the actions that stemmed from it, and information gaps that remain. Provide feedback to those involved in the intelligence process as to what was most helpful and why, and suggestions for further improvement.

IV. Auditing and Purging Files

With time, many intelligence files become little more than historical accounts of unit activity. Over time, intelligence files may no longer be accurate, relevant to the mandates of the unit, or pertain to current intelligence unit interests and activities, or they may contain insufficient supporting documentation. When files are deficient in one or more of these areas, agencies may consider updating or improving them through validation and other means. However, when

[37] For more information, see "RISSIntel," criminal intelligence database, https://www.riss.net/rissintel/.

[38] In the U.S., examples include the National Institute of Standards and Technology (NIST), the National Information Exchange Model (NIEM), the National Identity Exchange Federation (NIEF), and the Global Federated Identity and Privilege Management (GFIPM) program.

[39] UN Office on Drugs and Crime, *Criminal Intelligence Manual for Analysts* (2011), 10–16, https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf.

the basic information contained in these files is of such an age or of such poor quality as to make these efforts either too costly or unproductive, a decision to purge the files may be the most prudent approach.[40] Auditing intelligence files can help identify files to be purged. In addition, an annual review of all procedures and processes should be conducted to ensure continuing compliance with the criteria established by regulation or program policy.

Agencies with sufficient resources may consider using an external auditor. Use of a qualified and experienced outside auditor is often considered the best approach to purging intelligence files in that independent third parties remove much of the bias or the appearance of bias that may be evident when using in-house intelligence personnel. However, in many agencies, these audits are conducted internally.

The governing agency is responsible for purging and auditing intellignece files on a regular basis in accordance with applicable regulations. While a yearly review of the files for purposes of purging useless materials is recommended, this does not preclude the destruction of files on an ad hoc basis where appropriate and with approval of the Intelligence OIC or designee. Regardless, agencies should articulate their procedures for purging information.

V. TRAINING

Training in the manner in which intelligence information may be gathered and the means for reporting that information should be provided to all operations personnel. Not only does this facilitate the intelligence function, but also it may serve to overcome misunderstandings about the nature and uses of intelligence among operational personnel.

Although standards may vary internationally, the U.S. Department of Justice provides Minimum Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States, with specific training objectives identified by role.[41] Additional resources include the Bureau of Justice Assistance's Criminal Intelligence Systems Operating Policies Online Training Program,[42] the National Criminal Intelligence Resource Center,[43] and the International Association of Law Enforcement Intelligence Analysts (IALEIA) Professional Certification Program.[44]

[40] In the U.S., 28 CFR § 23.20 specifies a retention period of no more than five years.

[41] U.S. Department of Justice, *Minimum Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States* (2007), **https://www.ncirc.gov/documents/public/Minimum_Criminal_Intel_Training_Standards.pdf**.

[42] Bureau of Justice Assistance, "Criminal Intelligence Systems Operating Policies Online Training Program," **https://28cfr.ncirc.gov/**.

[43] National Criminal Intelligence Resource Center, "Training," **https://www.ncirc.gov/Training.aspx**.

[44] IALEIA, "Professional Certification Program," **https://www.ialeia.org/certification_process.php** .

ADDITIONAL REFERENCES:

- Association of Law Enforcement Intelligence Units: **http://www.leiu.org/about**
- Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, Analysis Toolkit: **https://it.ojp.gov/AT**
- Canadian Security Intelligence Service: **https://www.canada.ca/en/security-intelligence-service.html**
- Criminal Intelligence Analysis – Interpol: **https://www.interpol.int/en/How-we-work/Criminal-intelligence-analysis**
- Criminal Intelligence Coordinating Council: **https://it.ojp.gov/global/working-groups/cicc**
- IACP, *Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing at the Local, State and Federal Levels*: **https://www.theiacp.org/sites/default/files/2018-08/CriminalIntelligenceSharingReport.pdf**
- International Association of Law Enforcement Intelligence Analysts, Intelligence Library: **https://www.ialeia.org/intelligence_library.php**
- David L. Carter, ed., *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies,* 2nd ed.: **https://it.ojp.gov/documents/d/e050919201-IntelGuide_web.pdf**
- Rich LeCates, "Intelligence-Led Policing: Changing in the Face of Crime Prevention," *Police Chief*: **https://www.policechiefmagazine.org/changing-the-face-crime-prevention**
- Patrick McGlynn and Godfrey Garner, *Intelligence Analysis Fundamentals*
- National Criminal Intelligence Resource Center: **https://www.ncirc.gov/**
- *National Criminal Intelligence Sharing Plan*, 2.0: **https://it.ojp.gov/GIST/150/National-Criminal-Intelligence-Sharing-Plan-Version-2-0**
- National Fusion Center Association: **https://nfcausa.org/**
- Police Foundation and the U.S. Department of Justice, Office of Community Oriented Policing Services (COPS), *Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders*: **https://cops.usdoj.gov/RIC/Publications/cops-w0690-pub.pdf**
- Regional Information Sharing System: **https://www.riss.net/**
- United Nations (UN) Office on Drugs and Crime, *Criminal Intelligence Manual for Front-Line Law Enforcement* **https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Front_Line_Law_Enforcement.pdf**
- UN Office on Drugs and Crime, *Criminal Intelligence Manual for Analysts*: **https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf**
- U.S. Department of Homeland Security, Homeland Security Information Network (HSIN): **https://www.dhs.gov/homeland-security-information-network-hsin**
- U.S. Department of Justice, *Navigating Your Agency's Path to Intelligence-Led Policing*: **https://it.ojp.gov/documents/d/Navigating%20Your%20Agency's%20Path%20to%20Intelligence-Led%20Policing.pdf**
- U.S. Director of National Intelligence, Intelligence Community Directive 203: Analytic Standards: **https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf**
- U.S. Office of National Drug Control Policy, High-Intensity Drug Trafficking Areas (HIDTA): **https://www.hidtaprogram.org/intelligence_centers.php**

International Association of Chiefs of Police
44 Canal Center Plaza, Suite 200
Alexandria, VA 22314
703.836.6767 | FAX 703.836.4743
www.theIACP.org