

**TITLE: CRIMINAL INTELLIGENCE**

**CODIFIED: 69.3**

**EFFECTIVE: 04/22/17**

**RESCINDS/AMENDS:**

**PAGES: 6**

### PURPOSE

It is the purpose of this policy to provide law enforcement officers in general, and officers assigned to the intelligence function in particular, with guidelines for the collection, analysis, and distribution of intelligence information.

### DEFINITIONS

*Criminal intelligence*- Information compiled, analyzed and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity.

*Human Intelligence*- Also known as HUMINT, this is the gathering of information from human sources. Interrogation, confidential informants, confidential sources would be classified under this heading.

*Law Enforcement Sensitive (LES)* - meaning it should not be disseminated or discussed outside of law enforcement channels.

*Open Source*- Open Source Intelligence, often referred to as OSINT, is defined as any intelligence produced from publicly available information that is collected, exploited, and disseminated in timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement.

*Reasonable Suspicion*— “Reasonable suspicion” (or, criminal predicate) is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative department officer, investigator, or employee a basis to believe that there is a reasonable possibility that an

individual or organization is involved in a definable criminal activity or enterprise.” *US Department of Justice, Code of Federal Regulations 28 Part 23.20(c)*.

*Right to Privacy*- The right to be left alone, in the absence of some reasonable public interest in gathering, retaining, and sharing information about a person’s activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating a person’s privacy.

*Rapid Intelligence Technology Teams*- Conduct parallel investigation utilizing technological solutions to support the primary unit, provide support for the primary investigative unit, and focus on locating the suspect(s) rapidly using specially trained staff (collateral assignment).

*Strategic Intelligence*- Information concerning existing patterns or emerging trends of criminal activity designed to assist criminal apprehension and crime control strategies, for both short and long-term investigative goals.

*Suspicious Activity*- is “observed behavior reasonably indicative of preoperational planning related to criminal activity.” Examples of suspicious activity include surveillance, photography of facilities, site breach or physical intrusion, cyber- attacks, testing of security, etc.

*Suspicious Activity Report (SAR) Information*- Official documentation of observed behavior reasonably indicative of preoperational planning related to criminal activity. Suspicious activity report (SAR) information offers a standardized means for feeding information repositories or data analysis tools. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support inter-department calls for service.

*Tactical Intelligence*- Information regarding a specific event that can be used immediately by the operational units to further a criminal investigation, plan tactical operations and provide for officer safety.

*Threshold for criminal intelligence-* The threshold for collecting information and producing criminal intelligence shall be the “reasonable suspicion” standard in 28 CFR, Part 23, Section 23.3 c.

## POLICY

Information gathering is a fundamental and essential element in the all-encompassing duties of any law enforcement department. When acquired, information is used to prevent crime, pursue and apprehend offenders, and obtain evidence necessary for conviction. It is the policy of this department to gather information directed toward specific individuals or organizations where there is reasonable suspicion (as defined in 28 CFR, Part 23, Section 23.3 c) 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 department, all members of this department are responsible for reporting information that may help identify criminal conspirators and perpetrators.

1. Information gathering in support of the intelligence function is the responsibility of each member of this department although specific assignments may be made as deemed necessary by the officer-in-charge (OIC) of the intelligence authority.
2. Information that implicates, suggests implication or complicity of corruption shall be immediately reported to this department’s Chief of Police or another appropriate department.

It is also the policy of this department that if this department performs an intelligence function, procedures must be established to ensure the legality and integrity of its operations, to include.

- Procedures for ensuring information collected is limited to criminal conduct and

relates to activities that prevent a threat to the community;

- Descriptions of the types or quality of information that may be included in the system;
- Methods for purging out-of-date or incorrect information; and
- Procedures for utilization of intelligence personnel and techniques.

The policy contained herein is intended to remain at all times consistent with current language of 28 CFR, Part 23.

## PROCEDURE

### A. Mission

It is the mission of the intelligence function to gather information from all sources in a manner consistent with the law and to analyze that information to provide tactical and/or strategic intelligence 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 department.

### B. Organization

Primary responsibility for the direction of intelligence operations; coordination of personnel; and collection, evaluation, collation, analysis, and dissemination of intelligence information is housed in this department’s intelligence authority under direction of the Criminal Investigations Division Captain and/or his /her designated intelligence OIC.

1. The OIC shall report directly to this department’s Criminal Investigations Division (CID) Captain in a manner and on a schedule prescribed by the CID Captain.

2. To accomplish the goals of the intelligence function and conduct routine operations in an efficient and effective manner, the OIC shall ensure compliance with the policies, procedures, mission, and goals of the department.
3. The intelligence analyst will report directly to the CID Captain.
4. The OIC/intelligence analyst will be assigned to the Criminal Investigations Division.

### C. Professional standards

The intelligence function is often confronted with the need to balance information-gathering requirements for law enforcement with the rights of individuals. To this end, members of this department shall adhere to the following:

1. Information gathering for intelligence purposes shall be premised on circumstances that provide a reasonable suspicion (*as defined in 28 CFR, Part 23, Section 23.3 c*) that specific individuals or organizations may be planning or engaging in criminal activity.
2. Investigative techniques employed shall be lawful and only so intrusive as to gather sufficient information to prevent criminal conduct or the planning of criminal conduct.
3. The intelligence function shall make every effort to ensure that information added to the criminal intelligence base is relevant to a current on-going investigation and the product of dependable and trustworthy sources of information. A record shall be kept of the source of all information received and maintained by the intelligence function.
4. Information gathered and maintained by this department for intelligence purposes may be disseminated only to appropriate persons for legitimate law enforcement purposes in accordance with law and procedures established by this department. A record

shall be kept regarding the dissemination of all such information to persons within this or another law enforcement department.

5. It will be the practice of personnel involved in the intelligence function to abide by the privacy policy as outlined in the Santa Fe Police Department directive.

### D. Compiling Intelligence

1. Intelligence analysis/files may be opened by the intelligence OIC with sufficient information and justification. 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 investigative steps to include proposed use of informants, photographic, or electronic surveillance;
  - c. resource requirements, including personnel, equipment, buy/flash monies, travel costs, etc;
  - d. anticipated results; and
  - e. problems, restraints or conflicts of interest.
2. Officers shall not retain official intelligence documentation for personal reference or other purposes, but shall submit such reports and information directly to the intelligence authority.
3. Information gathering using confidential informants as well as electronic, photographic, and related surveillance devices shall be performed in a legally accepted manner and in accordance with procedures established for their use by this department.
4. All information designated for use by the intelligence authority shall be submitted on the designated Request for Information report form and reviewed by the officer's immediate supervisor prior to submission.

**E. Analysis**

1. The intelligence function shall establish and maintain a process to ensure that information gathered is subjected to review and analysis to derive its meaning and value.
2. Where possible, the above-described process should be accomplished by professional, trained analyst.
3. Analytic material (i.e., intelligence) shall be compiled and provided to authorized recipients as soon as possible where meaningful trends, patterns, methods, characteristics or intentions of criminal enterprises or individuals emerge.

**F. Receipt/Evaluation of Information**

Upon receipt of information in any form, the OIC shall ensure that the following steps are taken:

1. Where possible, information shall be evaluated with respect to reliability of source and validity of content. While evaluation may not be precise, this assessment must be made to the degree possible in order to guide others in using the information. A record shall be kept of the source of all information where known.
2. Reports and other investigative material and information received by this department shall remain the property of the originating department, but may be retained by this department. Such reports and other investigative material and information shall be maintained in confidence, and no access shall be given to another department except with the consent of the originating department.
3. Information having relevance to active cases or that requires immediate attention shall be forwarded to responsible investigative or other personnel as soon as possible.
4. Analytic material shall be compiled and provided to authorized sources as soon as possible where meaningful trends, patterns, methods, characteristics, or intentions of criminal enterprises or figures emerge.

**G. File Status**

Intelligence file status will be classified as either "open" or "closed," in accordance with the following:

## 1. Open

Intelligence files that are actively being worked will be designated as "Open." In order to remain open, officers working such cases must file intelligence status reports covering case developments at least every 180 days.

## 2. Closed

"Closed" intelligence files are those in which investigations have been completed, where all logical leads have been exhausted, or where no legitimate law enforcement interest is served. All closed files must include a final case summary report prepared by or with authorization of the lead investigator.

**H. Classification/Security Intelligence**

1. Intelligence files will be classified in order to protect sources, investigations, and individual's rights to privacy, as well as to provide a structure that will enable this department to control access to intelligence. These classifications shall be reevaluated whenever new information is added to an existing intelligence file.

## a. Restricted

"Restricted" intelligence files include those that contain information that could adversely affect an-going investigation, create safety hazards for officers, informants, or others and/or compromise their identities. Restricted intelligence may only be released by approval of the Criminal Investigations Division Captain or the department's Chief of Police to authorized law enforcement agencies with a *need and right to know*.

b. Confidential  
 “Confidential” intelligence is less sensitive than restricted intelligence. It may be released to department personnel when a need and right to know has been established by the intelligence Criminal Investigations Division Captain or his/her designate.

c. Unclassified  
 “Unclassified” intelligence contains information from the news media, public records, and other sources of a topical nature. Access is limited to officers conducting authorized investigations that necessitate this information.

2. All restricted and confidential files shall be secured, and access to all intelligence information shall be controlled and recorded by procedures established by the intelligence OIC.

a. Informant files shall be maintained separately from intelligence files as outlined in directive 69.1.21, Confidential Informants.

b. Intelligence files shall be maintained in accordance with state and federal law.

c. Release of intelligence information in general and electronic surveillance information and photographic intelligence, in particular, to any authorized law enforcement department shall be made only with the express approval of the intelligence OIC and with the stipulation that such intelligence not be duplicated or otherwise disseminated without the approval of this department’s OIC.

d. All files released under the Inspection of Public Records Act (IPRA) or through disclosure shall be carefully reviewed.

e. Intelligence sharing will be disseminated on a *Need to Know and Right to Know* bases, which will be determined by the Criminal Investigations Division Captain or his/her designee.

#### **I. Auditing and Purging Files**

1. The OIC 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 shall be audited and purged in compliance with *28 CFR Part 23* and as established by the department and through an independent auditor.

2. When a file has no further information value and/or meets the criteria of any applicable law, it shall be destroyed. A record of purged files shall be maintained by the intelligence authority.

#### **J. Notification of Criminal Intelligence and Analysis Unit**

The Criminal Intelligence and Analysis unit will be notified of immediate/potential threats to the community to include, but not limited to the following:


- Human Trafficking
- Large seizures of narcotics
- Large seizures of currency
- Large seizures of weapons
- Bomb threats
- Threats to infrastructures
- Active shooter
- Immediate/potential threats of mass casualties

- Suspicious activity at educational and governmental facilities
- Suspicious activity near monumental landmarks
- Hazardous material incidents
- Transnational gang activity
- Local gang activity
- Transnational and Domestic Organized Crime
- Domestic Terrorism
- Serial crimes against persons
- Organized Crime
- Drug Trafficking Organizations

---

DRAFTED (rfv) 03/17

Approved:

  
**PATRICK G. GALLAGHER**  
Chief of Police

Date:

4/25/17