



**DEPARTMENT OF PUBLIC SAFETY
POLICIES & PROCEDURES**



POLICY NUMBER	
OPR:02	
EFFECTIVE DATE: 02/24/2011	ORIGINAL ISSUED ON: 06/15/1989
REVISION NO: 2	

SUBJECT: INTELLIGENCE COLLECTION

1.0 PURPOSE

It is the purpose of this policy to establish guidelines and procedures for the collection, storage, analysis, and dissemination and utilization of intelligence information.

2.0 POLICY

It is the policy of this Department to gather information regarding suspected criminal activity or activities that pose a threat to citizens or their communities, to gather it with due respect for the rights of those involved, and to disseminate it only to authorized individuals. All members of this agency are responsible for reporting information that may help identify criminal conspirators and perpetrators.

3.0 APPLICABILITY

This policy applies to all commissioned employees and criminal analysts of the Department of Public Safety.

4.0 REFERENCES

- A. Code of Federal Regulations 28 CFR, Part 23B. §14-2-1, Right to Inspect Public Records; Exceptions, NMSA 1978
- B. §29-10-4, Confidentiality of Arrest Records, NMSA 1978
- C. CALEA Chapter 42 – Criminal Investigation

5.0 DEFINITIONS

- A. **Criminal Intelligence** – Information compiled, analyzed and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity.
- B. **Strategic Intelligence** – Information concerning existing patterns or emerging trends of criminal activity designed to assist in criminal apprehension and crime control strategies, for both short- and long-term investigative goals.
- C. **Tactical Intelligence** – Information regarding a specific criminal event that can be used immediately by operational units to further a criminal investigation, plan tactical operations and provide for officer/public safety.

6.0 PROCEDURE

A. Overview

- 1. Information gathering in support of the intelligence function is the responsibility of each member of this agency although specific assignments may be made as deemed necessary by the Office of the Chief.

2. Information that implicates, suggests implication or complicity of any public official in criminal activity or corruption shall be immediately reported to the Office of the Chief.
3. Criminal intelligence may only be collected on an individual, group, organization or business if;
 - a. It is believed that the subject of the criminal intelligence may be involved in criminal activity; and
 - b. The criminal intelligence may be relevant to that criminal activity.

B. Organization

1. Although the Department of Public Safety does not operate an intelligence component and/or fusion center, operational units within the Law Enforcement Program are capable of submitting intelligence reports through the New Mexico Criminal Justice Information System (CJIS). Additionally, intelligence reports may be submitted to the NM All Source Intelligence Center Liaison or submitted directly to the Center at *intelligence.fusion@state.nm.us*.
2. For intelligence information submitted into CJIS, primary responsibility for the evaluation, submission, analysis, and dissemination of intelligence information is the responsibility of the originator of such information. However, this does not preclude a commissioned officer from requesting assistance, which may include analysis of information, from a criminal, investigative support analyst assigned to the Investigations Bureau.
3. Requests for criminal, investigative support from the criminal analysts must be made in writing to the Investigations Bureau commander or his designee. The request must include the type of assistance needed, a summary of the investigation, and relevant timelines, i.e., trial dates.

C. Professional Standards

Intelligence efforts are often confronted with the need to balance information-gathering requirements for law enforcement with the rights of individuals. Therefore, members of this Department shall adhere to the following:

1. Information gathering for intelligence purposes shall be based on circumstances that provide a reasonable indication that a crime has been committed or is being planned, or on activities that present threats to communities.
2. Investigative techniques employed shall be lawful and only so intrusive as to gather sufficient information to prevent the criminal act and/or to identify and prosecute violators.
3. Intelligence efforts shall include every attempt to ensure that information added to the criminal intelligence base (CJIS) is 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 respective bureaus.
4. Information gathered and maintained by the DPS for intelligence purposes may be disseminated only to appropriate persons for legitimate law enforcement purposes in accordance with 28 CFR, Part 23. A CJIS record shall be kept regarding the

dissemination of all such information to persons within this or another law enforcement agency.

5. Certain information is specifically excluded from being collected as part of the criminal intelligence function. This excluded information includes:
 - a. Information about an individual or group merely on the basis that the individual or group supports controversial causes.
 - b. Information on an individual or group merely on the basis of ethnic background.
 - c. Information on an individual or group merely on the basis of religious or political affiliations.
 - d. Information on an individual or group merely on the basis of non-criminal personal habits.

D. Compiling Intelligence

1. Officers shall not retain official intelligence information for personal reference or other purposes but shall submit such reports and information directly to CJIS or the NM All Source Intelligence Center.
2. 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 Department policies *OPR:19 Use of Recording Equipment, OPR:39 Criminal Investigations, OPR:40 Crime Scenes*.
3. All information designated for use by the intelligence group shall be submitted on the designated report form (CJIS) and reviewed and approved by the officer's immediate supervisor.

E. Receipt/Evaluation of Intelligence Information

1. Upon receipt of information in any form, the receiving officer's immediate supervisor shall ensure that the following steps are taken:
 - a. 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 confidential source of all information where known. The confidential source and content shall be rated in accordance with the following:

	Source	Content
High	Completely Reliable	Confirmed as True
Medium	Fairly Reliable	Possibly True
Low	Reliability Unknown	Truth Unknown

Unknown	Reliability Questionable	Truth Questionable
---------	--------------------------	--------------------

- b. Reports and other investigative material and information received by this agency shall remain the property of the originating agency. Such reports and other investigative material and information shall be maintained in confidence, and no access shall be given to another agency except with the written consent of the originating agency.
- c. Information having relevance to active cases or that requires immediate attention shall be forwarded to responsible investigative or other personnel as soon as possible.
- d. Analytic material shall be compiled and provided to authorize sources as soon as possible where meaningful trends, patterns, methods, characteristics or intentions of criminal enterprises or figures emerge.

F. Intelligence Status

- 1. Intelligence status shall be classified as either “open” or “closed,” in accordance with the following:
 - a. **Open:** Intelligence that is 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.
 - b. **Closed:** Intelligence is that 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 the authorization of the lead investigator.

G. Classification/Security of Intelligence

- 1. Intelligence will be classified in order to protect sources, investigations, as well as to provide a structure that will enable this agency to control access to intelligence. These classifications shall be reevaluated whenever new information is added to existing intelligence.
 - a. **Restricted:** Includes information that could pose demonstrable and serious harm to an existing or contemplated criminal prosecution or an on-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 Investigations Bureau commander or the chief to authorized law enforcement agencies.
 - b. **Unclassified:** Includes intelligence that 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 information shall be secured, and access to all intelligence information shall be controlled and recorded in accordance with the following procedures.

- a. All intelligence shall only be submitted into CJIS, through the Intelligence module in CJIS.
- b. The Information Technology Division shall maintain the system and restrict access to the intelligence function to authorized users. Users must be vetted by the Investigations Bureau commander or his/her designee and must be trained in 28 CFR, Part 23.
- c. Informant files shall be maintained separately from intelligence files and in accordance with state and federal law.
- d. Release of intelligence in general and electronic surveillance information and photographic intelligence, in particular, to any authorized law enforcement agency shall be made only with the express approval of the Investigations Bureau commander and with the stipulation that such intelligence not be duplicated or otherwise disseminated without written approval from the Department.
- e. All information released under IPRA or ARIA or through disclosure shall be carefully reviewed.
- f. Department personnel are prohibited from using criminal intelligence for personal gain, political purposes or any purpose other than in the fulfillment of official law enforcement duties.

H. Auditing and Purging Information

1. The Investigations Bureau chief is responsible for ensuring that all information are maintained in accordance with the goals and objectives of the Department and include information that is both timely and relevant. Therefore, all intelligence shall be audited and purged on an annual basis in accordance with the following procedure.
 - a. Out-of-Date Information: The information Technology Division shall electronically purge information older than 5 years based on the "Last Update Date."
 - b. Incorrect Information: When incorrect information is found, the Investigations Bureau commander or his designate, shall immediately notify the originator of the information about the inaccuracy. The originator shall be given 10 days to correct the information and be informed that it will be purged if it is not corrected within the deadline.
2. Intelligence sent to the NM All Source Intelligence Center shall be compliant with 28 CFR, Part 23.

I. Annual Review

1. The commander of the Investigations Bureau, Department of Homeland Security and/or designee will be responsible for conducting an annual review of the intelligence collection process and all applicable procedures. This analysis should also look at recommendations for improved training, equipment, and/or policy changes, as necessary. The annual review shall be submitted to the Office of the Chief no later than the last day of January following the year to be reviewed. A copy of the analysis shall also be submitted to the Research and Development Section of the Standards Bureau for CALEA accreditation purposes.

7.0 ATTACHMENTS

NONE

8.0 APPROVAL

APPROVED BY: s/Gorden E. Eden Jr
DPS Cabinet Secretary

DATE: February 24, 2011