Peoria Police Department Policy and Procedure Manual

Policy 5.02
Criminal Intelligence

**"Our Community…
Our Commitment"**

I. POLICY

It is the policy of the Peoria Police Department to provide for an information base that meets the needs of the Department in carrying out its efforts to protect the public and suppress criminal operations. These standards are designed to bring about an equitable balance between the civil rights and liberties of our citizens and the needs of law enforcement to collect and disseminate criminal intelligence on the conduct of persons and groups who may be engaged in systematic criminal activity. (51.1.1.a)

II. DEFINITIONS

A. Active Gang Member: While this group is comprised of less than 20% of the total gang population, it is responsible for the greatest percentage of violent gang related crime and is considered to be the most violent and dangerous. This group is identified by documenting two (2) of the six (6) categories contained in the Gang Membership Identification Criteria (GMIC) list.

B. Associate: This group comprises the largest membership of the gang population is identified by documenting one (1) of the six (6) categories contained in the GMIC list.

C. Criminal Intelligence Information: Data which has been evaluated to determine that it is relevant to the identification of, and the criminal activity engaged in by, an individual who, or an organization which, is reasonably suspected of involvement in criminal activity.

D. Criminal Activity: any activity, which violates state statutes, ordinances, or codes and constitutes a criminal act under the law (excluding traffic violations).

E. Gang Member Identification Criteria (GMIC): A structured format consisting of six (6) categories used for the purpose of identifying a subject's gang affiliation as well as to document this information for potential legal hearings.

F. GIMIC Card: A hard copied form, which is disseminated by the Department of Public Safety and used as a means of obtaining consistent information to collaborate a subject's gang affiliation.

G. Intelligence System: The arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange, or dissemination and analysis of criminal intelligence information.

H. Need to Know: defined as the necessity to obtain or receive criminal intelligence information in the performance of official duties and responsibilities as a law enforcement or criminal justice authority.

I. Reasonable Suspicion or Criminal Predicate: is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise.

J. Right to Know: is defined as the legal authority to obtain or receive criminal intelligence information pursuant to court order, statue or decisional law.

K. Street Gangs: An active organization, association, or group of three (3) or more individuals (formal or informal), who form together for the purpose of committing criminal acts.

L. Validation of Information: means the procedure governing the periodic review of criminal intelligence information to assure its continuing compliance with system submission criteria established by this policy.

M. Working Confidential Intelligence File: that information which does not readily meet the minimum threshold for reasonable suspicion or criminal predicate, but with the approval of the Criminal Intelligence/Homeland Security Analyst or designee, may be held for a period not to exceed twelve months for the purpose of further investigation to corroborate the information to meet the minimum threshold.

N. 28 CFR Part 23: The purpose of this Federal Regulation is to assure that all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968 are utilized in conformance with the privacy and constitutional rights of individuals.

III. PROCEDURE

A. Criminal Intelligence File: Administration and coordination of the Criminal Intelligence File will be the ultimate responsibility of the Criminal Intelligence/Homeland Security Analyst. (11.1.1)

1. Intelligence Activities: Intelligence activities performed by the Peoria Police Department shall include:

a. The gathering of information from reliable sources (informants), as well as those who have not been corroborated (citizens).

b. Analyzing the value, quality, and reliability of information received.

c. Dissemination of the information to the proper departmental components.

2. File Contents: To ensure the protection of innocent persons, it is imperative that the legality and integrity of the Department's intelligence effort be continually monitored for compliance with applicable state statutes and federal regulations. (51.1.1.a)

a. The Criminal Intelligence/Homeland Security Analyst will review all intelligence information and ensure that all information meets intelligence criteria before authorizing its entry into the Criminal Intelligence File Database. Types of information that may be targeted for entry into the intelligence file may include, but are not limited to: (11.1.1) (51.1.1.a & b)

(1) Major crimes that have been committed in the area.

(2) Narcotics activity which has been validated, or there is "reasonable suspicion" of drug activity.

(3) Movements and locations of known or suspected criminal suspects.

(4) Gang related activity and identification.

(5) All sex offenders who reside in the City of Peoria or immediate surroundings, who may pose a threat to the public.

b. No information will be entered into the Criminal Intelligence File Database except upon specific approval by the Criminal Intelligence/Homeland Security Analyst responsible for coordination of the files.

c. No intelligence data will be gathered, collected, or maintained on religious, political, racial, ethnic, or sexual information which does not relate to criminal conduct or suspect identification and associations with individuals, which may not be of a criminal nature.

B. All intelligence files and the intelligence system will be maintained in accordance with 28 CFR Part 23.

C. Authorized Intelligence Information: The Criminal Intelligence Files provides for the addition, deletion, or updating of the following information:

1. Control Officer.

2. Date of Entry.

3. Name of person making entry.

4. Type of intelligence file.

5. Names, addresses, DOB's, and other physical and Departmental information.

6. Associates names, addresses, DOB's, and other physical and Departmental information.

7. Aliases.

8. Vehicle Information.

9. Information Sources.

10. Release information, documentation, and tracking.

11. Purging and deletion.

12. Narrative.

13. Related Cases.

D. Information Sources: Information sources must be protected to maintain their reliability, safety, and future usefulness.

1. A Department informant who provides information will be referred to by their Confidential Informant (CI) number within the information sources section of the Criminal Intelligence File.

2. Citizens desiring to provide information will be listed by name within the information source section of the Criminal Intelligence File.

a. If the person providing information does not want to be named in any forthcoming inquiry or investigation based on the information they provide, this will be annotated in the disposition narrative within the information source section of the Criminal Intelligence File.

b. If the citizen will not provide their identity at the time the information is received, "concerned citizen" will be selected under the source type within the information source section of the Criminal Intelligence File.

c. All informant and citizen information sources will be referred to as "confidential sources of information" within the narrative section of the Criminal Intelligence Files.

3. Any information received and entered into the Criminal Intelligence File must have the source and content reliability verified and given a classification.

a. Source Reliability

(1) Reliable – The reliability of the source is unquestionable or has been well tested in the past.

(2) Usually Reliable – The reliability of the source can usually be relied upon as factual. The majority of information provided in the past has proven to be reliable.

(3) Unreliable – The reliability of the source has been sporadic in the past.

(4) Unknown – The reliability of the source cannot be judged. Its authenticity or trustworthiness has not yet been determined by either experience or investigation.

b. Content Reliability

(1) Confirmed – The information has been corroborated by an investigator or another independent, reliable source.

(2) Probable – The information is consistent with past accounts.

(3) Unknown – The information is inconsistent with past accounts.

(4) Undetermined – The information cannot be judged. Its authenticity has not yet been determined by either experience or investigation.

(5) Cannot be Judged – Its authenticity has not yet been determined by either experience or investigation.

c. Classification

(1) Sensitive – Information pertaining to significant law enforcement cases currently under investigation, corruption of government officials or other sensitive information.

(2) Confidential – Confidential intelligence information which is not designated sensitive or information obtained through intelligence unit channels that is not classified sensitive and is for law enforcement use only.

(3) Restricted – Information that at an earlier date was classified sensitive and the need for high-level security no longer exists or non-confidential information prepared for/by law enforcement agencies.

(4) Unclassified – Civic related information to which, in its original form, the general public had direct access (i.e. birth and death certificates), new media information, newspaper, magazines and periodical clippings dealing with specified criminal categories.

E. Submission, Retention, and Purging:

1. Intelligence information will be submitted to the Criminal Intelligence/Homeland Security Analyst for potential inclusion into the intelligence files by the following methods:

a. Memorandum detailing the intelligence information.

b. Field Interview Card completed as outlined in Policy 4.01.

c. Police Reports.

d. Intelligence Report Form.

2. The employee receiving intelligence information will be responsible for submitting the information.

3. The Criminal Intelligence Files will contain:

a. The written communications on the information noted in section D.1.

b. Data Review and Dissemination Log

c. The Cover Sheet

d. C.I. File Face Sheet

e. Any other information associated with the corroboration of the minimum threshold except those items identified as public records.

4. Intelligence files will be color coded to designate their status:

a. Blue files will designate working intelligence files.

b. Red files will designate active intelligence files.

5. A Master Log will be maintained designating the Intelligence File number given to each case along with the purge date.

6. Retention and Purging of Information. All Criminal Intelligence files will be retained and maintained in accordance with the guidelines established in 28 CFR Part 23. (51.1.1.c)

a. Working Criminal Intelligence File: Information regarding suspected criminal activity which does not meet the minimum threshold may be retained for no longer than twelve (12) months.

b. Criminal Intelligence Files: To maintain the integrity of the system and the accuracy of the information while protecting the rights of citizens, criminal intelligence files will be retained for five (5) years.

(1) The purge date will be five (5) years from the date the information was entered into the criminal intelligence system.

(2) If there is further corroborated activity which meets the minimum threshold, this information must be documented in the file and this establishes a new purge time.

c. It is the responsibility of the Criminal Intelligence/Homeland Security Analyst to review the purge dates of each file and ensure that any purged documents are destroyed in such a manner so as to protect the interests of all involved by shredding the information.

F. Release of Criminal Intelligence Information

1. The Criminal Intelligence/Homeland Security Analyst shall organize and analyze intelligence information being received, and shall prepare and release intelligence reports to various Departmental components and outside law enforcement agencies on a need to know basis in accordance with the designated classification level. Intelligence information shall not be released if the disclosure of such information:

a. Interferes with an active investigation.

b. Constitutes an invasion of privacy.

c. Discloses the identity of a confidential source.

d. Discloses a confidential investigation technique or procedure.

e. Endangers the life or safety of a law enforcement officer.

2. The procedures for releasing intelligence information are as follows:

a. Request for Intelligence information that is forwarded to the Criminal Intelligence/Homeland Security Analyst shall be reviewed for value and the need to know pertaining to criminals or their criminal activity.

b. Intelligence information that is beneficial to currently active regional task forces shall be copied and personally delivered to the commanding officer of the specific task force involved. If the information is urgent, it will be telephoned to the appropriate task force supervisor, and a copy of the written documentation submitted to the file.

c. Information that is beneficial to other law enforcement agencies will be in written form and forwarded to the Criminal Intelligence/Homeland Security Analyst for dissemination through the DPS Intelligence System.

d. Information that is beneficial to other components within the Department shall be provided in the following methods:

(1) Confidential information releases.

(2) FI listings.

(3) Beat Profiles.

(4) Intelligence Bulletins.

(5) Verbally, when time is limited during an emergency.

G. Security of Criminal Intelligence Files:

1. Intelligence files shall be secured under lock and key, or in the event of computer files, be protected through password security as approved by the Rocky Mountain Information Network (RMIN) and the Chief of Police. All hard copies of criminal intelligence files will be retained in a location approved by the Chief of Police. (51.1.2)

2. Access to Criminal Intelligence Files for the purpose of adding, deleting, or modifying information shall be restricted to: (51.1.2)

a. The Criminal Intelligence/Homeland Security Analyst.

b. Others, as authorized by the Chief of Police.

3. Computer access to intelligence information shall be available only to Department employees who are trained to adequately search for information on a 24-hour a day, need to know basis.

a. The RISS accessible computers within the Department, except for the Criminal Intelligence/Homeland Security Analyst computer, will be utilized for query ONLY.

b. The Criminal Intelligence/Homeland Security Analyst computer will be the ONLY computer within the Department for data input into the Regional Information Sharing System (RISS) criminal intelligence data system.

4. Those reviewing the intelligence files must do so in a place designated by the Criminal Intelligence/Homeland Security Analyst.

5. All individuals accessing the intelligence file must be logged into the Data Review and Dissemination Log.

6. All Criminal Intelligence files contained in a computer system will be backed up by a hard copy file.

H. Gang Operations

1. The Criminal Intelligence/Homeland Security Analyst shall have the responsibility of organizing and coordinating all gang intelligence information.

2. Objectives

a. To inhibit and dispel involvement in street gang memberships through the strategic break-down of gang activity patterns.

b. To reduce the violence associated with street gangs.

c. To reduce community fears generated by the presence of street gangs.

d. To reduce the destructive effect of gang activity resulting in substantial monetary loss to the citizens of the City of Peoria.

3. Responsibilities (51.1.1.b)

a. Patrol Officers:

(1) Assist in the collection and identification of gang intelligence.

(2) Assist the Gang Intelligence Coordinator and SCU, as needed, in the course of their normal duties.

b. Gang Intelligence Coordinator:

(1) Function as the Peoria Police Department expert on street gangs.

(2) Collect, arrange, interpret and disseminate, through the chain of command, all gang intelligence.

(3) Conduct in-service training for Department employees on gangs as needed. Investigate gang/gang related crime as assigned.

(4) Prepare and conduct public gang awareness presentations as requested by the Community Services Supervisor.

(5) Attend various valley meetings on gangs as appropriate.

4. Procedures:

a. Identification of Gang Member Intelligence

(1) Officers from each shift shall be assigned to coordinate all gang intelligence information for their respective shifts.

(2) Extreme caution must be taken by all personnel in remaining objective in their observations of persons suspected of gang membership or affiliation.

(3) Only those individuals who can be documented as gang members or associates will be included in the Department gang files.

(4) Photographs will be taken of documented active gang members.

(5) Associate gang members may be photographed by a Gang Intelligence Officer or at their direction by another sworn officer, with the associate member's consent.

(6) The following guidelines may be used when attempting to determine a subject's gang involvement (other factors may apply):

(a) Self proclamation.

(b) Witness testimony (official statements).

(c) Correspondence written/electronic).

(d) Paraphernalia and photographs.

(e) Tattoos.

(f) Clothing/colors.

(7) Prior to identifying an individual as an active gang member, two (2) or more of the above factors must be present. An individual meeting one (1) of the above elements may be identified as an associate member.

(8) Upon notification of gang related information, officers will complete a gang information card and take at least two (2) photographs of any previously identified active gang members or associate gang members in accordance with paragraph 4.a.(4)/(5) of this order (unless the member(s)/associate(s) specifically refuse to be photographed when asked for consent). The officer will photocopy the gang information card and will forward the original card and photographs to the Gang Intelligence Coordinator. Any other information, such as fingerprints, information obtained from other agencies, etc., will be forwarded to the Gang Intelligence Coordinator. It is the responsibility of officers and the Gang Intelligence Coordinator to ensure that anyone recorded on a gang information card meets the previously established criteria, reflected in Paragraph 4.a.

(9) The Gang Intelligence Coordinator may periodically publish a confidential list of identified gang members/associates on the Mobile Data Computer (MDC) Intelligence Section. This list shall be treated with the strictest of confidence and shall not be made available for public disclosure.

(10) All gang files will be classified as Criminal Intelligence Information and be maintained in accordance with the guidelines established in this policy.

(a) Active Gang Files will be maintained for a period of five years from the date of documentation on the GMIC card or re-documentation.

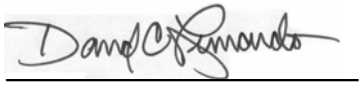
(b) Associate Gang files will be maintained in the same manner as working intelligence files and be maintained for a period of 12 months from the date of documentation on the GMIC card.

I. Intelligence Operations

1. To maximize the value of intelligence information gathered by this and other agencies, the Criminal Intelligence/Homeland Security Analyst shall develop and maintain a liaison with applicable federal, State, and local agencies for the exchange of intelligence information. This exchange may be through informal channels, or through formal meetings of persons involved in the intelligence function.

2. Information Dissemination: The Criminal Intelligence/Homeland Security Analyst shall ensure that applicable intelligence information is being distributed to the various Departmental components as needed. Intelligence information shall be distributed to Department personnel on the approved Department form, "Confidential Information Only to Law Enforcement Personnel" or Intelligence Bulletins.

Peoria Police Department
Policy 5.02 Criminal Intelligence
Original Issue Date: 01/01/03
Last Revision Date: 02/10/06
Next Review Date: 09/30/07
Office of Primary Responsibility: TSB
Editor: M. Self
Reviewed By: K. Ashley

APPROVED: 

David C. Leonardo
Chief of Police