CRIMINAL INTELLIGENCE

Date of Issue **NOVEMBER 29, 2001**	*General Order Number* **01-08**
Effective Date **February 7, 2017**	*Section Code* **INV-03**
Reevaluation Date **March 2019**	*Amends / Cancels*
C.A.L.E.A. **42.1.6, 46.3.1, 46.3.2, 82.3.5**	*Reference*

INDEX AS:

Criminal Intelligence
Intelligence
Intelligence Reliability
Inspections

I. PURPOSE

The purpose of this order is to identify the purposes for which criminal intelligence may be obtained, the purpose for which it may be used, who may access the information and methods for identifying the reliability of the information. In addition the order identifies the security and maintenance requirements for housing intelligence files and procedures for the dissemination of information contained in the files.

II. POLICY

It is the policy of the Iowa City Police Department to identify those types of criminal activity, which require intelligence information beyond the normal practices of the department. All information submitted to Intelligence files shall be obtained in legal manner, verified to the extent practical and reviewed on a regularly scheduled basis and disseminated only to serve a legitimate law enforcement purpose.

III. DEFINITIONS

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

Reasonable Suspicion - is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency 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.

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.

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 safety.

IV. PROCEDURES

All agency personnel have a role in criminal intelligence and the sharing of information. While the collection of intelligence is necessary to successfully combat criminal activity, the collection of this type of information must conform to federal, state and local requirements. The collection of intelligence data is only permitted to fulfill a criminal investigation purpose and intelligence data shall be purged from the system when it no longer serves a useful purpose. Access to intelligence files shall be limited to the Chief of Police or designee, Commander of Field Operations, Commander of the Investigative Section and others as determined by the Commander of the Investigative Section on a case by case basis. Personnel submitting information to the intelligence system will be allowed access to the file associated with the information as needed.

The commander of the Investigative Section is responsible for the evaluation, housing, maintenance, security, and dissemination/re-dissemination of strategic intelligence information. Only those personnel specifically mentioned above will have direct access to strategic intelligence files. Any officer or outside agency requesting intelligence information from the system shall direct their request to the Commander of the Investigative Section.

The inclusion of information obtained from organizations, i.e. LEIN, or through participation in multi-jurisdictional task force shall comply with these requirements.

The Commander of Investigations in consultation with the Chief of Police or designee will determine the need for gathering criminal intelligence and the means by which this information will be obtained. Personnel used in obtaining intelligence information will be familiar with the techniques and devices to be used for the collection of intelligence.

FOCUS OF STRATEGIC INTELLIGENCE ACTIVITIES

Members of the Iowa City Police Department shall only collect strategic intelligence information concerning an individual where there is "reasonable suspicion" that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.

The collection of Strategic Criminal Intelligence shall be for the purpose of suppressing criminal activity in the Iowa City area. The types of incidents for which intelligence information may be obtained include, but are not limited to:

1. Narcotics manufacturing and/or trafficking;
2. Unlawful gambling;
3. Extortion;
4. Vice and pornography;
5. Infiltration of businesses for illegitimate purposes;
6. Bribery;
7. Major crime including homicide, burglary, auto theft, kidnapping, destruction of property, robbery, fraud, forgery, fencing of stolen property and arson;
8. Manufacture, use, or possession of explosive devices for fraud, intimidation or political reasons;
9. Organized crime;
10. Corruption of public officials;
11. Threats to public officials and private citizens;
12. Traveling criminals;
13. Gang activities;
14. Other designated multi-jurisdictional activities.

SUBMISSION OF INFORMATION

Information submitted for inclusion in strategic intelligence files shall clearly identify the focus of the investigation. This shall include but not be limited to as many of the following identifiers that are available:

1. Full name;
2. Date of Birth;
3. Address;
4. Aliases;
5. Social Security number;
6. Drivers License number;
7. Physical Description; (height, weight, eye and hair color)
8. Place of birth;
9. Citizenship (if alien, Identification Number)
10. Distinguishing scars, marks, or tattoos;
11. Violence potential;
12. Criminal identification number;
13. Criminal associates;
14. Modus Operandi.

The collection of strategic intelligence information about the political, religious, or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization, is prohibited unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.

Submitted information shall include:

1. Date of submittal;
2. Name of submitting officer;
3. Name of submitting agency/organization.

EVALUATION OF INFORMATION

Prior to entry in to the strategic intelligence system, the Commander of the Investigative Section shall evaluate the information. The evaluation shall include the reliability of the source of the information and the strength/validity of the information. Only information whose reliability and validity had been evaluated will be entered in the system. I.e. if reliability is unknown and the validity cannot be judged, it will not go in the system, as it would not meet the reasonable suspicion standard.

Reliability shall be evaluated as follows:

1. Reliable - the reliability of the source is unquestioned or has been well tested in the past.
2. Usually reliable - the reliability of the source can usually be relied upon.
3. Unreliable - the reliability of the source has been sporadic in the past.
4. Unknown - the reliability of the source cannot be judged; authenticity or trustworthiness has not yet been determined by either experience or investigation.

Validity shall be evaluated as follows:

1. Confirmed - the information has been corroborated by an investigator or another reliable independent source.
2. Probable - the information is consistent with past accounts.
3. Doubtful - the information is inconsistent with past accounts.
4. Cannot be judged - the information cannot be judged. Its authenticity has not yet been determined by either experience or investigation.

DISSEMINATION/RE-DISSEMINATION OF INFORMATION

Request for information from strategic intelligence files shall be directed to the commander of the investigative section. The request shall contain the name of the person requesting the information, the date, time and purpose of the request. In addition the request should identify specific identifying information on the person for whom the information is being requested.

The Chief of Police or designee, Commander of Field Operations, Commander of Administrative Services or Commander of Investigations may distribute

information contained in intelligence files to members of the Iowa City Police Department or other law enforcement agencies. Information disseminated from intelligence files shall be designated as such. Members of this department are prohibited from forwarding or re-disseminating information from intelligence files to persons outside the Iowa City Police Department without the express permission of the Chief of Police or designee, or Commander of Field Operations, or Commander of Administrative Services or Commander of Investigations.

When information from strategic intelligence files is disseminated, the Commander of Investigations shall record the following information within the file:

1. The date of dissemination of the information;
2. The name of the individual requesting the information;
3. The name of the agency/organization requesting the information;
4. The reason for the release of information; (need to know/right to know)
5. The information provided to the requester;
6. The name of the person disseminating the information.
7. The submission of intelligence information to regional or national criminal intelligence databases shall be in conformance with 28 CFR.

TERRORISM RELATED INFORMATION

The Iowa City Police Department shall maintain a liaison with other organizations for the exchange of information related to terrorism. This liaison may be in the form of direct contact with specific departments and/or through such organizations as MOCIC, Iowa Homeland Security, United States Homeland Security, LEIN and the Iowa Fusion Network. The Commander of Field Operations or designee shall be responsible for the dissemination of terrorist related information within the department and shall approve the re-dissemination of terrorist related information to other organizations. When appropriate, such information shall be in the form of a written report accompanied by supporting documentation.

REVIEW AND PURGING PROCEDURES

Review and purging of intelligence information should be an ongoing process. The maximum retention period for intelligence information is five (5) years. If the information has not been updated and/or validated within the past 5 years, the information shall be purged from the intelligence files. IF information has been updated within the past five years, the file may be retained for a period of five (5) years from the most recent entry.

Material purged from intelligence files shall be thoroughly deleted from any electronic storage devices and/or hard copies shall be shredded or otherwise made unusable. A record of the purge may be maintained containing the date and reason of the purge, as well as the name of the person completing the purge.

The Chief of Police or designee may periodically inspect the intelligence file system to ensure that safeguards and requirements are being met. On an annual basis the Commander of Investigations shall review the policy and procedures of the criminal intelligence function to ensure compliance and effectiveness. Agency personnel shall

receive initial training in the criminal intelligence function and refresher training at least once every three years.

Jody Matherly, Chief of Police

WARNING

This directive is for departmental use only and does not apply in any criminal or civil proceeding. The department policy should not be construed as a creation of a higher legal standard of safety or care in an evidentiary sense with respect to third-party claims. Violations of this directive will only form the basis for departmental administrative sanctions.