

# Florida State University Police Department



CRIMINAL INTELLIGENCE		
Revision Effective Date:	General Order 813	Attachments: None
09/05/17		
Rescinds/Amends: 13-26	Distribution: Department Wide	CFA Reference:
(04/01/14), 09-26		19.01 – 19.02
	Pages: 5	

# **Policy - Criminal Intelligence Policy**

It is the policy of the FSU Police Department (FSU PD) to gather, correlate, analyze, and disseminate information from within the Department and other law enforcement agencies concerning criminal suspects and activities. Moreover, the gathering and dissemination of criminal intelligence information shall comply with all pertinent state and federal laws.

#### **Procedures**

# A. Policies Concerning Intelligence Information

FSU PD members shall report intelligence information regarding known criminals, suspects, and activities posing a criminal threat. Intelligence information shall be submitted to the Investigations Section when such information is not otherwise contained within an incident report.

- Intelligence information shall be reduced to writing and submitted to the Support Services
   Captain or the designated Intelligence Officer. The Intelligence information shall be
   appropriately noted whether the source was verified, determined to be reliable, and/or whether
   the information was verified.
- 2. The submitting officer shall make every effort to list the source and motive for providing the information.
- 3. The Assistant Chief designated Intelligence Officer shall ensure that the submitted information is from a reliable source and is limited to criminal conduct or relates to activities that present a serious threat to the community [CFA 19.01 A.].

## B. **Authority and Responsibility**

The intelligence function shall operate under the authority of the Chief of the FSU PD and be assigned as a function of the Investigations Section. The Support Services Captain shall be responsible for reporting to and keeping the Chief informed of intelligence activities. In addition:

- 1. Personnel shall be assigned for specific circumstances dependent upon the evaluation of the intelligence information and the totality of the circumstances.
- 2. Intelligence functions shall include, but not be limited to:

- a. Gathering information and identifying criminals, criminal activity, organized criminal groups, and crime patterns.
- b. Collating and disseminating information within the Department and to external agencies.
- c. Establishing and maintaining liaison with other local, state, and federal agencies.
- 3. The intelligence function shall include maintaining membership in state and regional intelligence groups as allowable by available funding.

### C. Collection of Intelligence Data

The collection of intelligence data is the primary step in the intelligence process.

- 1. Raw data/information will be collected from a variety of sources, including, but not limited to:
  - a. Media publications.
  - b. Official police reports.
  - c. Criminal intelligence submissions from officers.
  - d. Other law enforcement agencies.
  - e. Confidential informants.
  - f. Public records.
  - g. Citizens.
  - h. Other records gathered by legal methods.
- 2. Once the raw data has been collected, it will be subjected to collation and analysis to determine the accuracy of the information.
- 3. The collection of intelligence data/information directly related to a particular investigation or criminal activity shall be conducted utilizing a variety of methods, depending on existing conditions. Overt methods include [CFA 19.01 B.].
  - a. Public records.
  - b. Official police reports.
  - c. Media publications.
  - d. Criminal intelligence data bases.
- 4. Covert methods include [CFA 19.01 B.].
  - a. Undercover or decoy operations.
  - b. Confidential informants.
  - c. Surveillance, including ground, aerial, and electronic means. See the General Order titled, "Surveillance, Decoy, and Undercover Operations."
  - d. Photography or video recording.
  - e. Binoculars or night vision equipment.
  - f. Analytical investigation.
  - g. Court-ordered wire intercepts.
  - h. Other methods meeting established, legal guidelines.

### D. Evaluation of Intelligence Data

All intelligence data and information evaluated and reviewed by the Support Services Captain and/or designated Intelligence Officer shall be subjected to careful scrutiny for reliability and accuracy of content.

- 1. To ensure uniformity, the following guidelines are for the general evaluation of intelligence data and shall be used according to the following definitions [CFA 19.01 C.].
  - a. Reliable—The reliability of the source is unquestioned or has been tested in the past.
  - b. Usually Reliable—The reliability of the source can usually be relied upon to be factual. The majority of information in the past has proven to be reliable.
  - c. Somewhat Reliable—The reliability of the source has been sporadic in the past.
  - d. Unable to Judge—The reliability of the source cannot be judged. The authenticity or trustworthiness has not been established by either experience of investigation.
- 2. Content Validity [CFA 19.01 C.].
  - a. <u>Factual</u>—The information has been corroborated by independent source(s).
  - b. Possibly True—The information is consistent with past accounts.
  - c. Doubtful—The information is not consistent with past accounts.
  - d. Accuracy Unknown—The information cannot be evaluated for its validity.
- 3. How Obtained [CFA 19.01 C.].
  - a. <u>Views of Source</u>—Source actually witnessed the occurrence/activity.
  - b. Hearsay to Source—The source heard the information and is related what was heard.
  - Unknown—The method used by the source to obtain the information is not known or documented.

## E. Analysis of Intelligence Data

The analytical process of intelligence will include various types of reports, intelligence briefs, crime control evaluation projects, and intelligence assessments utilizing data from a variety of sources.

- 1. All investigative analysis reports will indicate the source of information from which the data was obtained.
- 2. An evaluation will be made to evaluate the source of the information as to accuracy and validity. Attempts will be made to substantiate the information through other sources. All analyses of intelligence data shall be conducted in a secure environment. That is, such analyses will not be conducted in any non-secured space or in the presence of individuals without a need to know or members of the general public [CFA 19.02 A].

# F. Prohibited Intelligence Practices

The intelligence function shall recognize the delicate balance between the individual rights of citizens and the legitimate needs of law enforcement. In order to provide proper internal safeguards to ensure these rights are not violated, or the democratic process subverted, the following practices are prohibited.

- 1. Intelligence data will not be collected by any member of the FSU PD merely on the basis that a certain person supports unpopular causes, unless criminal intent can be shown.
- 2. Intelligence data will not be collected on any person merely on the basis of ethnicity or race. See the General Order titled, "Prohibition Against Bias-Based Profiling."
- 3. Intelligence data will not be collected on any individual merely on the basis of the individual's religious and/or political affiliation.
- 4. Information shall not be gathered by any employee or his or he agent by illegal or unlawful means.
- 5. No member of the FSU PD will use intelligence data for political and/or economic purposes.

## G. Dissemination of Intelligence Data

Dissemination guidelines regarding the release of information are necessary to ensure the integrity of the intelligence function. The Chief or designee may authorize intelligence information to be released.

- 1. Information receiving proper authorization for release and is classified as public records in accordance with Section 119.07, F.S., shall be coordinated through the Public Information Officer (PIO) or designee.
- 2. Information may be released to the following:
  - a. Duly-constituted law enforcement agencies at a federal, state, or local level once the identity of the requester has been ascertained [CFA 19.02 B].
  - b. The general public and news media may receive information concerning the arrest of individuals or matters of an investigation that are public record(s).
- 3. Information relating to an on-going and active criminal investigation is not subject to release to the media or general public.

#### H. Security Measures to Protect Intelligence Data and Files [CFA 19.02 B and C]

The security of information contained within the intelligence files is necessary to ensure the integrity of the entire intelligence function, the confidentiality of the information, and the protection of individuals' privacy rights. Breaches in security can seriously undermine the intelligence process. Thus, the intelligence files shall be maintained under the control of the Support Services Captain or designated Intelligence Officer.

- 1. Access to the files are limited to:
  - a. Chief.
  - b. Major
  - c. Support Services Captain
  - d. Intelligence Officer
  - e. Other sworn members upon approval by the Support Services Captain.
- Officials from duty-constituted law enforcement agencies authorized to review the intelligence files shall do so only in the presence of the Support Services Captain\_or designated Intelligence Officer.
- 3. Intelligence files shall remain secured when not under the direct control of the Support Services Captain or designated Intelligence Officer.

- 4. All files and intelligence data shall be secured in a locking file cabinet inside the Investigator's Office who, as the Intelligence Officer has been authorized by the Support Services Captain to maintain the data. For electronic data, such data shall be secured in a password-protected database [CFA 19.02 D.].
- 5. All discarded paper material shall be shredded. Investigative products no longer useful or which cannot be legally retained shall be destroyed.

# I. Purging and Destruction of Intelligence Files [CFA 19.01 D.]

Intelligence information shall be purged and shredded, or electronically deleted, in accordance with the General Records Schedule for Law Enforcement Agencies, as authorized by Chapters 119 and 257, F.S.

- 1. Data and information no longer needed to support the intelligence function shall be purged, shredded, electronically deleted, or destroyed.
- 2. Data and files determined to contain incorrect information shall be purged, shredded, or electronically deleted immediately.
- 3. Data will be purged from intelligence files and indices after a five-year period and/or if the files meet one or all of the following conditions:
  - a. The data is no longer relevant or necessary to the mission and objectives of the FSU PD.
  - b. The data has become obsolete and cannot be utilized for any present and/or future strategic or tactical intelligence purpose.

# **Glossary**—None

#### Index

Criminal Intelligence Files Records, Criminal Intelligence Intelligence Officer

Attachments: None

MTC 09/01/17 Filed: General Order 813

Title: Criminal Intelligence

Approved: David L. Perry, Chief

Date: 09/01/17