SOUTH MIAMI
POLICE DEPARTMENT

GENERAL ORDER NUMBER: 24.1	DATE OF ISSUE: July 31, 2011	EFFECTIVE DATE: May 14, 2014	NUMBER OF PAGES: 05
CFA STANDARD: 19 SUBJECT: Criminal Intelligence- ADMINISTRATION	NEW (X) RESCINDS ( ) AMENDS ( ) OTHER ( )	By Order Of: *Rene Landa,* *CHIEF OF POLICE*	

CFA STANDARD: 19.01M, 19.02M

SECTIONS:

24.1.1 Safeguard Procedures

24.1.2 Records, Storage and Security

RESCINDS: All existing orders in conflict.

PURPOSE: To establish departmental policy for the gathering, analysis, and dissemination of intelligence information; to provide procedures for collecting and purging intelligence information; to provide guidelines for the use of special investigations funds for intelligence gathering; to establish procedures for intelligence file maintenance and security.

SCOPE: All departmental employees.

POLICY: It is the policy of the South Miami Police Department to use all lawful means to collect, process, and disseminate intelligence information relating to criminal activities, subversive activities, vice activities, terrorism, and civil disorders for the purpose of identifying and controlling these activities within the community.

PROCEDURE:

24.1.1 Safeguard Procedures

A. The Criminal Investigations Division will be responsible for intelligence activities, for ensuring that the information collected is limited to criminal conduct and relates to activities that present a threat to the community; and for the maintenance of intelligence files. All officers acquiring intelligence concerning criminal activities will submit such information, through their chain of command, to the Criminal Investigations Division for appropriate action. [CFA19.01(A)]

B. Any departmental employee receiving information relating to criminal conduct or other functions and responsibilities of the CID should document the information. Except information concerning illegal /unethical employee conduct, the documented information will be delivered to the CID via chain of command, for analysis and appropriate action. Information concerning employee conduct will be handled in accordance with General Order No. 25 (Internal Affairs).

C. The collection of raw intelligence data is the primary step in the intelligence process; it is here the intelligence function will begin to detect the occurrences of organized criminal activity within its jurisdiction, surrounding area, and the State. The raw data will be collected from a variety of sources including, but not limited to, the following:

1. Media publications;
2. Official police reports;
3. Criminal intelligence submissions from officers;
4. Other law enforcement agencies;
5. Confidential informants;
6. Public records; and
7. Other records gathered via legal methods.

The CID Lieutenant will designate one or more detectives to receive intelligence information, collate and analyze the data, determine its accuracy, identify subjects involved, and determine the presence of criminal activity. This information will then be dispersed to the appropriate unit (GIU, SIU) for enforcement action. The CID Supervisor will also ensure that the originator of the information receives feedback at the appropriate time, and recognition, if warranted.

D. Procedures for maintaining legality and integrity:{CFA 19.01(b)}

1. The collection of criminal intelligence information concerning particular individuals, businesses, and hate or subversive groups or enterprises, is restricted to criminal conduct and will be related to activities that present a threat to the community. The information may be collected and maintained only:

   a. If evidence exists connecting individuals with known or suspected criminal activity; and
   b. If the information is relevant to that criminal activity.

2. To ensure that informants are secure in their anonymity, the procedures outlined in General Order 19.2, Section 19.2.9 will be used when dealing with informants.

3. The following are procedures for the utilization of intelligence personnel, equipment, and techniques: [CFA19.01(c)]

   a. Requests for the utilization of the intelligence function may be made via telephone, fax, in writing, or in person to the Detective Bureau Supervisor. After analysis, the CID Lieutenant will evaluate the request and present the information to the Chief of Police to determine whether to handle it departmentally, or in cooperation with another agency.

   b. Required surveillance or electronic equipment will be checked out by the CID Lieutenant to the individual detective requesting it, as available;

   c. Electronic surveillance and wire intercepts may only be conducted after approval by the Chief of Police, and in accordance with provisions of Florida State Statute 934. The CID Lieutenant will ensure that statutory regulations are adhered to;

   d. Photographic surveillance or video recordings may be conducted to identify any and all person(s), either as members or associates of groups or organized criminal enterprises, or as members of a terrorist organization who engage in or are suspected of illegal activity; and to provide evidence of any illegal activity.

4. Evaluation of Intelligence Data: All intelligence data/information to be evaluated and reviewed will first be subjected to careful scrutiny for reliability and accuracy of content.

5. To ensure uniformity within the intelligence function, the following guidelines are adopted for the general evaluation of intelligence data: [CFA19.01(b)]

   a. <u>Source Reliability</u>:
      1) Highly Reliable - The reliability of the source is unquestioned or has been tested to be reliable in the past;
      2) Unknown Reliable - The reliability of the source may or may not be relied upon as factual. The majority of information provided in the past has proven to be reliable;
      3) Somewhat Reliable - The reliability of the source has been sporadic in the past;
      4) Unable to Judge - The reliability of the source cannot be judged. The authenticity or trustworthiness has not been established by either experience or investigation.

b. How Obtained:

1) On View - Source actually witnessed the occurrence/activity;

2) Hearsay - Source heard the information and related what was heard;

3) Unknown - The method used by the source to obtain the information is not known or documented.

6. Purging out-of-date Information: If the information proves inaccurate and the subject is not linked to known criminals or criminal activities or non-criminal in nature, it will be purged from the system without delay. The CID Lieutenant will review the intelligence files at least annually, and purge information that is no longer valid, active, current or useful. [CFA19.01(d)]

D. Accounting of Funds

1. Funds for the purpose of purchasing evidence, information and supporting other intelligence operations may be allocated from the Investigations Fund, as outlined in General Order 7.4, Section 7.4.1.

2. The CID Lieutenant is the custodian of the Investigations Fund. The fund is audited (G.O. 7.4.3) annually, or when the custodian changes, by the Chief of Police.

E. Intelligence Equipment: The CID maintains an inventory of specialized equipment (G.O. 20.1.4) for intelligence gathering. The equipment may only be used in accordance with the guidelines established in that order. No person may use any intelligence equipment unless they have demonstrated the ability to safely, properly and legally use the device. All use will be carefully documented.

24.1.2 Records, Storage and Security

The security of information contained in intelligence files is necessary to ensure the integrity of the intelligence process, the confidentiality of the information, and the protection of the individual's right to privacy. Breaches in security can seriously undermine the intelligence process. Unauthorized release of information contained in the intelligence files can jeopardize undercover operations and/or operatives, identify confidential sources, and threaten ongoing criminal investigations. For these reasons, security of intelligence data/files is imperative.

A. Intelligence records will be maintained under the control of the CID Lieutenant in the custody of the SIU. Intelligence records are maintained in a secure area within

the Detective Bureau and are kept separate from other police records. [CFA19.02(d)] The guidelines listed below are to eliminate unauthorized access to intelligence data/files:

1. Access to intelligence files (whether electronic or paper form) will be limited to the following personnel: [CFA19.02(b)and (c)]

    a. Chief of Police;
    b. Assistant Chief;
    c. Operations Bureau Captain
    d. CID Lieutenant;
    e. Detectives.
    f. Accreditation Manager

2. Certain intelligence information is considered of such a confidential nature that access will be restricted only to those personnel with a "Need to Know." Information designated as "Confidential - Need to Know" by the Chief of Police, or the CID Lieutenant, will be strictly maintained. Access to electronic files, will be limited to only those personnel listed above. The "Confidential - Need to Know" information will not be released to others without prior approval of the Chief of Police.

B. Collation and analysis of intelligence data will be done in a secure environment. The files of the intelligence function will remain secured when not under the direct control of CID personnel. All unattended files and intelligence data will be secured. No files or intelligence data will be left unsecured on desks at any time. [CFA19.02(a)] All discarded paper material will be shredded. Investigative products that are no longer useful or cannot be legally retained, such as those stored on video and audio tapes, CD, DVD, or diskettes, will be destroyed and all labels removed or obscured in order to prevent identification of subjects.

C. Those persons from other law enforcement agencies authorized to review the intelligence files will do so only in the presence of, and accompanied by, CID personnel. [CFA19.02(b)]