SEMINOLE COUNTY SHERIFF'S OFFICE GENERAL ORDER	NUMBER: G - 60
	RESCINDS:
SUBJECT:	**Criminal Intelligence**
EFFECTIVE:	**October 11, 2012**
REVISED:	**July 23, 2015**

Table of Contents:

I. PURPOSE:

This directive provides policy, guidelines and principles for the collection, analysis and distribution of intelligence information.

II. POLICY:

A. Information gathering is a fundamental and essential duty of law enforcement agencies, which may be used to prevent crime, pursue and apprehend offenders, and obtain evidence necessary for successful prosecution. It is Sheriff's Office policy to gather information on specific individuals and organizations if there is reasonable suspicion (as defined by 28 CFR, Part 23.3 c) that such individuals or organizations may be planning or engaging in criminal activity, that it be gathered with respect for the rights of those involved, and to only disseminate it to authorized persons. While the collection of criminal intelligence may be assigned to specific employees, and not just to those assigned to the Domestic Security Division (hereafter Domestic Security), all employees are responsible for reporting information that may help the Sheriff's Office identify criminal conspirators and perpetrators.

B. It is also Sheriff's Office policy to adopt the standards of the Commission on Accreditation for Law Enforcement Agencies (CALEA) for intelligence gathering, specifically: If an agency performs an intelligence function, procedures must be established to ensure the legality and integrity of its operations, to include:

1. Procedures for ensuring information collected is limited to criminal conduct and relates to activities that present a formal threat to the community,

2. Descriptions of the types or quality of information that may be included in the system,

3. Methods for purging out-of-date or incorrect information,

4. Procedures for the use of intelligence personnel or techniques.

C. This directive will remain consistent with the current language of 28 CFR, Part 23.

III. 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 crime trends that is designed to assist in the development of criminal apprehension and crime control strategies, conjunctive with Sheriff's Office short and long-term investigative goals.

C. *Tactical Intelligence:*
Information regarding a specific criminal event that can be immediately used by operational units to further a criminal investigation, plan tactical operations, or provide for officer safety.

D. *Threshold for Criminal Intelligence:*
The threshold for collecting information and producing criminal intelligence shall be the "reasonable suspicion" standard of 28 CFR, Part 23.3(c).

IV. PROCEDURES:

A. *Mission:*
It is Domestic Security's mission to gather information in a manner consistent with law, and to analyze it for tactical and/or strategic intelligence regarding the existence, identity and capability of suspects and criminal enterprises, and to use such information to further crime prevention and enforcement initiatives of the Sheriff's Office.

1. Information gathering in support of the intelligence function is the responsibility of each employee, although specific assignments may be made by the Division Captain.

2. Information that implicates, or suggests implication or complicity, of any public official in criminal activity or corruption shall be immediately reported to the Sheriff.

B. *Organization:*
Primary responsibility for the conduct of intelligence operations, the coordination of personnel, and the collection, evaluation, collation, analysis, and/or dissemination of intelligence information is that of Domestic Security.

1. The Division Captain shall collaborate with agency command staff to determine the manner and frequency in which intelligence products will be disseminated.

2. To accomplish the goals of the intelligence function, and to conduct routine operations in an

efficient and effective manner, the Division Captain shall ensure compliance with the policies and procedures, mission and goals of the Sheriff's Office.

C. *Operational Standards:*
The intelligence function is often confronted with the need to balance information-gathering requirements for law enforcement with the rights of individuals. To this end employees shall adhere to the following:

1. Information gathering for intelligence purposes shall be premised on circumstances that provide a reasonable suspicion (as defined in 28 CFR, Part 23.3(c)) that specifies that individuals or organizations may be planning or engaging in criminal activity.

2. Investigative techniques shall be employed in lawful manner and will only be so intrusive as to gather sufficient information to prevent criminal conduct or the planning of such conduct.

3. As is reasonably possible, the intelligence function shall make every effort to ensure that information added to the criminal intelligence base is relevant to an on-going investigation and is the product of dependable and trustworthy sources of information.

4. Intelligence information possessed by the Sheriff's Office may only be disseminated to appropriate persons, where there is a need to know and a right to know the information, for the performance of a law enforcement activity in accordance with law and Sheriff's Office procedures.

D. *Compiling Intelligence:*

1. Intelligence investigations files may be accessed by Domestic Security Detectives with sufficient information and justification. This includes, but is not limited to, the following types of information:

   a. Subject, victim, and complainant information as appropriate; summary of suspected criminal activity,

   b. Anticipated investigative steps to include proposed use of informants, photographic, or electronic surveillance,

   c. Resource requirements including personnel, equipment, buy/flash monies, travel expenses,

   d. Anticipated results, and

   e. Problems, restraints, or conflicts of interest.

2. Before accessing intelligence files, Detectives must complete a summary of their intended investigation and submit it to their supervisor for approval.

3. Deputies/ Detectives shall not retain intelligence information for personal use or other unauthorized purpose, but shall submit such reports and information directly to the Domestic Security Division.

4. Information gathering using confidential informants or electronic, photographic, or related surveillance devices or techniques shall be conducted in a legally accepted manner and in accordance with Sheriff's Office procedures.

5. All information designated for the use of Domestic Security shall be submitted by the Deputy/

Detective and reviewed by a Domestic Security Supervisor.

E. *Analysis:*

1. Domestic Security maintains a process to ensure that collected information is subjected to review and analysis to derive its meaning and value.

2. When possible, the above-described process should be accomplished by a combination of Analysts and Detectives.

3. Analytic material (i.e. intelligence) shall be compiled and provided to authorized recipients as soon as possible if meaningful trends, patterns, methods, characteristics, or intentions of criminal enterprises or suspects emerge.

F. *Receipt/Evaluation of Information:*
Upon receipt of information in any form, the chain of command in Domestic Security ensures the following procedural steps are taken:

1. When possible, information shall be evaluated with respect to source reliability 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. When known, records shall be kept of the information source.

2. Reports, investigative materials, and information received by the Sheriff's Office shall remain the property of the originating agency, but may be retained by the Sheriff's Office. This material shall be maintained in confidence, and no access shall be given to another agency except with the consent of the originating agency (Third Agency Rule).

3. Information having relevance to active cases or that which requires immediate attention shall be forwarded to responsible Detectives (or other authorized personnel) as soon as possible.

4. Analytic material shall be compiled and provided to authorized personnel as soon as possible if meaningful trends, patterns, methods, characteristics, or intentions of criminal enterprises or suspects emerge.

G. *File Status:*
Intelligence files will be classified as either "open" or "closed" in accordance with the following:

1. *Open:*
Intelligence files that are actively being worked will be designated as "open." To remain open, Detectives working these cases must file intelligence status reports addressing case developments every 180 days.

2. *Closed:*
Closed intelligence files are those in which investigations have been completed, where all logical leads are exhausted, or when no legitimate law enforcement interest is served. Closed files must include a final case summary report prepared by, or with the authorization of the lead Detectives, and reviewed by the Domestic Security Captain (or designee).

H. *Classification/Security of Intelligence:*

1. Intelligence files will be classified to protect sources, investigations, and an individual's right of privacy, as well as provide a structure that will enable the Sheriff's Office to control access to the information. Classifications are re-evaluated whenever new information is added to an existing intelligence file.

   a. *Command Confidential:*
   These files include those that contain information that could adversely affect on-going investigations or create safety hazards for officers, informants or other persons, and/or compromise their identities. Restricted intelligence may only be released on approval of the Domestic Security Captain or the Sheriff to authorized law enforcement agencies with a need and right to know.

   b. *Law Enforcement Sensitive (LES):*
   This intelligence is less sensitive than Command Confidential intelligence. It may be released to agency personnel when a need and a right to know are established by the Domestic Security Captain (or designee).

   c. *For Official Use Only (FOUO):*
   This intelligence contains information from the media, public records, or from other "open source" records. Access is limited to Deputies or other officials participating in or conducting authorized investigations that necessitate access to this information.

2. Command Confidential and Law Enforcement Sensitive files are secured, with access to it controlled as prescribed by procedures established by the Domestic Security Captain.

   a. Informant files shall be maintained separately from intelligence files.

   b. Intelligence files shall be maintained in accordance with Chapter 119, Florida Statutes, and 28 CFR, Part 23, Federal Regulations.

   c. The release of intelligence information 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 Domestic Security Captain, and with the stipulation that such intelligence not be duplicated or otherwise disseminated without the Captain's approval.

   d. Files to be released under freedom of information provisions or through disclosure shall be carefully reviewed before they are released.

I. *Auditing and Purging Files:*

1. The Domestic Security Captain is responsible for ensuring that files are maintained in accordance with the goals and objectives of the division and that they include information both timely and relevant. To ensure this occurs, all intelligence files are audited and purged on an annual basis as established by the Captain in accordance with state law and federal regulations.

2. If files have no further informational value and they meet the disposal criteria of applicable laws, they shall be destroyed. A record of purged files shall be maintained by Domestic Security.