



ANDERSON COUNTY
SHERIFF'S OFFICE

GO - 215

GENERAL ORDERS

CRIMINAL INTELLIGENCE

PURPOSE:

This policy establishes guidelines for collecting, processing, and disseminating information relating to specified crimes and criminal activities. Areas of concern typically include organized crime, illegal drug trafficking, terrorism, gangs, and civil disorders.

CRIMINAL INTELLIGENCE:

DEFINED – The end product of a process that converts individual items of information either into evidence or, more often, into insights conclusion, or assessments, perhaps less solid than fact but always more helpful than raw information, that can form the basis for the development of law enforcement strategies, priorities, policies, or investigative tactics regarding specific crime, suspect, criminal organization, etc. The intelligence process includes the systematic collection of raw information, which after collation, evaluation, and analysis, is disseminated to appropriate units of the agency.

ACCOUNTABILITY:

The Narcotics Unit of Special Operations is the central repository for intelligence records. Special Operations evaluates intelligence information, and arranges meetings to share and analyze information with affected division commanders, unit supervisors and investigators as needed.

The Division Commander of any Sheriff's Office component or function that gathers intelligence information is responsible for that activity within his division including compiling, initial evaluation and accountability of records. Intelligence records are then forwarded to Special Operations-Narcotics Unit.

NOTE: *All personnel are encouraged to gather criminal intelligence information and all relevant information is to be forwarded to the Narcotics Unit as soon as practicable.*

CRIMINAL INTELLIGENCE FILES:

A criminal intelligence file consists of stored information on the activities and associations of individuals and groups known or suspected to be involved in criminal acts or in the threatening, planning, organizing or financing of criminal acts. **More specifically, this stored information relates to individuals who fall into one or more of the following:**

1. Currently involved in or suspected of being involved in the planning, organizing, financing, or commission of criminal activities
2. Have threatened, attempted, planned, or performed criminal acts
3. Have an established association with known or suspected crime figures
4. Organizations and businesses involved in one or more of the following:

- Are currently involved in or suspected of being involved in the planning, organizing, financing, or commission of criminal activities; or
- Which have threatened, attempted, planned, or performed criminal acts; or
- Are operated, controlled, financed, infiltrated or illegally used by crime fighters.

**CRIMINAL
INTELLIGENCE
FILE CONTENT:**

Material stored in a criminal intelligence file is restricted to documents of criminal intelligence and related information from public records and media sources. Examples of excluded material are religious, political, or sexual information not relating to criminal conduct and associations with individuals not of a criminal nature.

**CRIMINAL
INTELLIGENCE
FILE CRITERIA:**

Criminal intelligences consist of two specific categories: **permanent files and temporary files.**

PERMANENT FILE – A file containing information pertaining to an identifiable subject meeting the following criteria justified for retention in a permanent criminal intelligence file:

1. Information which relates that an individual, organization, business or group is involved or suspected of being involved in one or more of the following criminal activities:
 - Narcotics trafficking
 - Unlawful gambling
 - Loan sharking
 - Extortion
 - Vice and pornography
 - Infiltration of legitimate business for illegitimate purposes
 - Stolen securities
 - Bribery
 - Threats to public officials and private citizens
 - Major fencing activities
 - Major crime including homicide, burglary, auto theft, kidnapping, destruction of property, robbery, fraud, forgery, and arson
 - Manufacture, use, or possession of explosive devices for purposes of fraud, intimidation, or political motivation
2. In addition to falling within the confines of one or more of the previously listed criminal activities, the subject entered into the permanent file is identifiable – distinguished by a unique identifying characteristic, e.g., date of birth, criminal identification number, or driver's license number. Identification at the time of file input is necessary to distinguish the subject from any similar individuals on file or any others to be entered at a later time.

TEMPORARY FILE – Information in file does not meet criteria for permanent file storage but has enough potential validity for the agency to want to retain it. It is recommended that retention of information in a temporary file not to exceed a one-year period unless compelling reason exists to extend this time period. During this period, efforts are to be made to identify the subject or validate the information so it may be transferred to the permanent file or destroyed. If the information still remains in the temporary file at the end of the one-year period, and compelling reason for its retention is not evident, the information is to be removed and destroyed. An individual, organization, business, or group may be given temporary file status in the following cases:

1. **Subject is unidentifiable.** Although suspected of involvement in criminal activities, the subject has no physical descriptors, identification numbers, or distinguishing characteristics available.
2. **Involvement is questionable.** Subject's involvement in criminal activities is questionable; however, based on one or both of the following reasons it would be beneficial to the agency to retain a record of the subject for a limited period of time during which the information can be validated.
3. **Possible criminal association.** Individual or organization, although not currently reported to be criminally active, associates with a known criminal and appears to be aided by abetting illegal activities.
4. **Criminal history.** Individual or organization, although not currently reported to be criminally active, has a history of criminal conduct and the circumstances currently being reported, i.e., new position or ownership in a business, affords an opportunity to again become criminally active.
5. **Reliability/validity unknown.** The reliability of the information source and/or the validity of the information cannot be determined at the time of receipt; however, the information appears to be significant and merits temporary storage while attempts are made to validate.

**INFORMATION
EVALUATION:**

Information retained in a criminal intelligence file is to be evaluated for source reliability and content validity prior to filing. The bulk of data in an intelligence file consists of allegations or information initially unverified. Evaluating the information's worth and usefulness is essential in protecting an individual's right of privacy. Circulating unreliable and invalid information is detrimental to agency's operations and contrary to an individual's right of privacy.

To ensure uniformity, the following terms describe language to be used in the evaluation process:

Source Reliability:

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 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 of trustworthiness has not yet been determined by either experience or investigation.

Content Validity:

1. **Confirmed** - The information has been corroborated.
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 evaluated.

FILE EVALUATION CODING SYSTEM – The following codes are to be noted on all file information to describe source reliability and content validity:

- Source Reliability - Note file information as: **Reliable, Usually Reliable, Unreliable, or Unknown.**
- Content Validity - Note file information as: **Confirmed, Probable, Doubtful, or Cannot be judged.**

**INFORMATION AND
DISSEMINATION
CLASSIFICATION:**

Information classification is the responsibility of a carefully selected and specifically designated individual in the effected operational unit. Information retained in a criminal intelligence file is to be classified to indicate the degree to which it will be kept confidential in order to protect sources, investigations, and an individual's right of privacy. Additionally, classification dictates the internal approval process to be completed prior to dissemination of the information to personnel outside the Sheriff's Office.

In order to ensure uniformity, the following diagrams the system to be used for classifying criminal intelligence files:

Security Class	Dissemination Criteria	Release Authority
Class I Confidential	Restricted to law enforcement intelligence personnel having a specific need-to-know and right-to-know	Division Commander
Class II Sensitive	Restricted to law enforcement intelligence personnel having a specific need-to-know and right-to-know	Unit Commander
Class III Restricted	Restricted to law enforcement personnel having a specific need-to-know and right-to-know	Unit Supervisor

DISSEMINATION – In order to protect the right of privacy of individuals contained in criminal intelligence files and to maintain confidentiality of sources and the file itself, the following applies to file dissemination:

- **NEED-TO-KNOW.** Requested information is pertinent and necessary to the requesting agency in initiating, furthering, or completing an investigation.
- **RIGHT-TO-KNOW.** Requesting agency has official capacity and statutory authority to the information requested.

To eliminate unauthorized use and abuse of criminal intelligence information, the following documentation is to be noted in disseminated files:

1. The name of the agency and individual requesting the information
2. The need-to-know clearly defined
3. The information provided
4. The name of the employee handling the request

Examples of classified information:

Class I – Confidential

- Information pertaining to law enforcement cases currently under investigation
- Corruption (police or other government officials)
- Informant identification information

Class II – Sensitive

- Criminal intelligence reports that refer to organized crime or terrorism
- Publications obtained through intelligence unit channels not deemed to be confidential

Class III – Restricted

- Reports that at an earlier date were classified confidential or sensitive and the need for high security no longer exists
- Non-sensitive reports published by local law enforcement agencies

DISSEMINATION – Information determined to be of a useful nature to operational units is to be disseminated in a timely manner. Supervisors are to solicit feedback to evaluate information effectiveness.

**INFORMATION
SOURCES:**

In a number of situations, the affected operational unit may elect to identify information sources for items stored in their criminal intelligence files. The value of information stored in a criminal intelligence file is often directly related to the source of the information.

Factors to consider in determining whether source identification is warranted include:

1. The nature of the information reported;
2. The potential need to refer to the source's identity for further investigative or prosecutorial activity; and
3. The reliability of the source.

When source identification is warranted, it will reflect the name of the agency and the individual providing the information. In cases where identifying the source is not practical for internal security reasons, a code number can be used. A listing of coded sources of information can then be retained by the operational unit commander. In addition to identifying the source, it may be appropriate in a particular case to describe how the source obtained the information, e.g., "S-60, a reliable police informant, heard" or "a reliable law enforcement source of the Anderson County Sheriff's Office saw" a particular event at a particular time.

In many cases there is no need to indicate the source of the stored information. However, each item of information is to be individually judged against established criteria to determine whether or not source identification is appropriate.

Deputies are encouraged to document information received from a variety of sources and training will emphasize that all personnel, regardless of their jobs, have a role in criminal intelligence gathering and the sharing of information. Deputies are also encouraged to take advantage of local and on-line training opportunities. Contact the Training Unit for additional information.

FILE PURGING:

Information stored in a criminal intelligence file is to be periodically reviewed and purged to ensure:

1. The file is current, accurate and relevant to the needs and objectives of the Sheriff's Office, and
2. To safeguard an individual's rights of privacy as guaranteed under federal and state laws.

Reviewing of criminal intelligence is to be done on a continual basis as personnel use the material in carrying out day-to-day activities. Information that appears to be no longer useful or cannot be validated is to be immediately purged from a file and destroyed.

To ensure review and purge of a file is conducted systematically, the following table outlines considerations required in the purge/destruction process:

Utility	Timeliness and Appropriateness	Accuracy and Completeness
How often is the information used?	Is the information outdated?	Is the information still valid?
For what purpose is the information being used?	Is the information relevant to the needs and objectives of law enforcement?	Is the information adequate for identification purposes?
Who uses the information?	Is the information relevant to the purpose for which it was collected and stored?	Can the validity of the data be determined through investigative techniques?
	Is the information available from other sources?	
	Is this non-intelligence information that should be stored elsewhere?	
	Is the security classification assigned the information still appropriate?	

PURGE TIME SCHEDULE – Review of criminal intelligence files for purging is to be conducted on an annual basis.

MANNER OF DESTRUCTION – Material purged from criminal intelligence files is to be destroyed under the supervision of members of the affected division commander.

**CRIMINAL
INTELLIGENCE
FILE SECURITY:**

Criminal intelligence files are to be located in a secure area with access restricted to authorized personnel. Physical security of criminal intelligence files is imperative to maintain confidentiality of the information stored and to ensure protection of an individual's right to privacy.

**DRUG EVIDENCE FOR
INVESTIGATIVE OR
TRAINING PURPOSES:**

These procedures will be followed when using drug evidence for investigative or training purposes:

1. The Unit Commander will submit a letter to the Division Captain and Sheriff requesting that seized drug evidence be allowed to be used in an operation/training. The letter will state the type and weight of narcotic to be used in the operation/training. When evidence is needed for an operation, an Operations Plan will be attached showing how the drug evidence will be used in an operation.
2. Upon final approval by the Sheriff, the case agent/handler will check out the drug evidence from the property and evidence section. The drug evidence will be weighed by the case agent/handler, property officer and a witness to show the approximate weight of the evidence. This will be documented by the property section and the case agent/handler will retain a copy for the case file.

NOTE: *Only evidence with a final disposition will be used, and the drug evidence should already have been tested by the Anderson-*

Oconee Regional Forensics Lab or the South Carolina Law Enforcement Division.

3. Upon receiving the drug evidence, the case agent/handler is responsible for the safeguard of the evidence until completion of the operation/training. If the evidence for an operation must be stored overnight, it will be kept in the narcotics agent's or handler's safe. Prior to placing in the safe and upon removal, the evidence shall be weighed again and witnessed to ensure that there is no discrepancy in weight of the evidence. No change in custody shall be permitted at any time, under any circumstances without approval of the Unit Commander, Division Captain or the Sheriff.
4. After the completion of the operation, the case agent/handler will return the evidence to the property and evidence section where the evidence shall be weighed by the agent/handler, property officer and a witness to ensure there is no discrepancy in the weight of the evidence. If any discrepancy is found, the Unit Commander shall be immediately notified and he shall immediately notify the Division Captain and Sheriff at that time.
5. The Unit Commander will notify the Division Captain and Sheriff immediately in the event any evidence has been lost, stolen, tampered with, or if any weight of the drug evidence can not be accounted for.

LIAISON:

To facilitate the effectiveness of intelligence gathering, the Sheriff's Office maintains a liaison with federal, state, and other local law enforcement agencies for the exchange of intelligence information.

TERRORISM:

The Sheriff's Office recognizes the need to quickly assess terrorism-related intelligence and direct that information to one or more organizations best suited to analyze and evaluate such information; therefore, the agency participates in the regional Joint Terrorism Task Force (JTTF) of the Federal Bureau of Investigation (FBI). The JTTF serves as liaison with other organizations for the exchange of terrorism-related information.

REPORTING – Deputies will use an incident report to document terrorism-related information. The report will be reviewed by a supervisor and forwarded to the appropriate investigator for follow-up and subsequent investigative supplementary.

RELAYING INTELLIGENCE – After receiving terrorism-related information, the investigator will determine if the information should remain in-house or be forwarded to a task force, other law enforcement agency or entity with a need-to-know.

If the investigator determines that information contained in the incident report and/or investigative supplementary is of a terrorist nature, the information will be forwarded to the appropriate task force, law enforcement agency or other entity as necessary based on a need and right-to-know.

In cases where an investigator is not available, or the information is extremely critical or time-sensitive, the on-call investigator or the on-call investigations supervisor will directly forward the information to the FBI via their 24-hour telephone number at (402) 493-8688.

AWARENESS INFORMATION – The Anderson County Sheriff's Office, in conjunction with Anderson County Emergency Services, is committed to providing terrorism awareness information to enable the public to identify and report terrorism-related information.

The Emergency Services Division, with input from the Sheriff's Office, will prepare public service announcements for local radio and television stations at times, and containing information, determined by the Sheriff, the Deputy Chief of Emergency Services, and/or the Joint Terrorism Task Force (JTTF).

The agency will maintain a citizen reporting form on the Sheriff's Office website to enable citizen reporting via the Internet.

ANNUAL REVIEW:

Intelligence-gathering activities are vital to the criminal intelligence function. As such, the Narcotics Unit Commander will provide an annual review of the agency's procedures and processes relative to the collection, processing, and sharing of intelligence information.

Approved by:
John S. Skipper, Jr., Sheriff