CHAPTER 51
CRIMINAL INTELLIGENCE

DISCUSSION: The purpose of this chapter is to provide guidelines for the collecting, processing, and disseminating of information relating to specified crimes and criminal activity. The criteria for the collection of criminal intelligence information is that there must be a reasonable and legitimate need to do so, and that information concerning political, religious, racial, or personal beliefs will not be collected or retained unless such information is relevant to a report of known or suspected criminal activity or presents a threat to the community.

51.1.1 Objectives of the Criminal Intelligence Function

A. To compile information files on members of the criminal element to establish probable cause for search and arrest warrants.

B. To maintain files on radical, subversive or clandestine groups, or organizations, which advocate the overthrow, disruption or destruction of Federal, State or Local Governments.

C. To maintain a record of any allegations, threats, intimidation and/or assaults on any officer, sworn official, or personnel.

D. To provide a basic source of information to the various divisions of the department which will assist in the over-all police function.

51.1.2 Responsibility and Reporting Procedures

A. In most cases information that would be considered intelligence will come to the attention of sworn officers, there may be occasions that such information may be discovered or reported to a non-sworn employee. It is the responsibility of all agency personnel that come across information that may be considered intelligence forward that information to the appropriate intelligence file manager.

B. The decision to initiate an intelligence report will be based upon the information and circumstances of each incident, generally involving the source of the information and the circumstances surrounding the incident. Each officer must make a decision on the basis of his/her knowledge of the person providing the information and/or his/her personal observation.

   1. Any person may submit an intelligence report anytime he/she receives intelligence information which might be in the interest of the Police Department, the Community, the State or the Federal Government.

   2. Any of the standard report forms, e-mail or memorandum style may be used and shall include the date and time the information was obtained.

3. The “Source and Information Rating Guide” is provided below to determine the credibility of the source/informant and the nature of information.

4. The first time that an individual's name appears in the body of the report, it should be in all upper case letters (CAPITALS). If it is used thereafter in the report, it may be in appropriate upper and lower case letters.

5. The report may be either handwritten or typed, as long as it is legible.

6. Details of the report should be a concise, but thorough synopsis of the facts. Officers should insure that critical information, i.e. names, times, places and figures are accurately recorded.

7. The report should be submitted directly to the intelligence file manager. If this is not possible, the submitter shall place the report in a sealed envelope, addressed and delivered to the appropriate file manager. Information of a "sensitive" nature should always be hand delivered.

C. Only information with a criminal predicate or activities that present a potential threat to the community and which meets the agency’s criteria for file input should be stored in the criminal intelligence files. Specifically excluded material includes:

1. Information on an individual or group merely on the basis that such individual or group supports unpopular causes.

2. Information on an individual or group merely on the basis of ethnic background.

3. Information on any individual or group merely on the basis of religious or political affiliations.

4. Information on an individual or group merely on the basis of non-criminal personal habits.

51.1.3 Source and Information Rating Code

The submitting officer shall use the “Source and Information Rating Code” to determine the credibility of his/her source/informant and the nature of the collected information. The submitting officer will make the determination of credibility based upon his/her knowledge of the person providing the information and/or his/her personal observation.

A. Information ratings guidelines.

1. Confirmation by other sources - Information is logical and confirmed by one or more reliable sources.

2. Probably true - Seems accurate, but has not been confirmed, and agrees with

other information on the same subject.

3. Possibly true - Information which has not been confirmed or contradicted; seems logical but not able to confirm; agrees with the general body of intelligence.

4. Doubtfully true - Information is unlikely to be true, but is not excluded; has not been contradicted or is totally illogical or incomplete disagreement with the general body of the intelligence of the subject.

5. Improbably report - Information is contradicted by other intelligence; is illogical and in disagreement with existing intelligence.

6. Truth cannot be judged - First time to receive information from subject, truth cannot be judged, lack of knowledge in information.

B. Source ratings guidelines

1. Completely reliable - There is no doubt that the person providing information is reliable and credible.

2. Usually Reliable - There may be some doubt that the person providing information is reliable and credible, but information received in the past has proven reliable in a certain number of cases.

3. Fairly Reliable - There is usually some doubt that the person providing information is reliable and credible; information received in the past has proven reliable in a certain number of cases.

4. Not Usually Reliable - There is doubt that the person providing information is reliable and credible; information received in the past has proven not reliable although reports have been submitted.

5. Unreliable - There is a great doubt that the person providing information is reliable and credible, past information has proven unreliable.

6. Reliability Cannot Be Judged - No way of knowing whether the person providing information is reliable or credible, first time to receive information.

51.1.4 Types of Files

Files are maintained and categorized in the following manner:

A. Criminal intelligence will be maintained, storage and managed by the Criminal Investigations Division.

B. Gang \ Narcotics intelligence will be maintained, stored and managed by the Special Operations Division.

C. Narcotics intelligence may also be submitted to and shared with METRO Narcotics multi-agency unit. While information is often shared between METRO agents and Hattiesburg Police officers, these intelligence files are maintained separate by METRO and are not part of the Hattiesburg Police department's intelligence filing and storage system. Any information submitted to METRO becomes the property of METRO and falls under their discretion as to the value, storing, purging or sharing of such information.

51.1.5 Purging of Records

General guidelines for reviewing and purging of information stored in the criminal intelligence file are as follows:

A. Utility

1. How often is the information used?

2. For What purpose if the information being used?

3. Who uses the information?

B. Timeliness and Appropriateness

1. Are investigations on going?

2. Is the information outdated?

3. Is the information relevant to the needs and objectives of the department?

4. Is the information relevant to the purpose it was collected?

C. Accuracy and completeness

1. Is the information still valid?

2. Is the information deemed adequate?

3. Is the data still relevant and useful?

D. Purging of records

1. Purging of information in the intelligence files is done on an ongoing basis as documents are reviewed using the guidelines in this directive.

2. Material purged from intelligence files shall be destroyed by shredding or incineration.

3. A written record shall be maintained of all items purged from intelligence files. This record can take the form of destruction order, a listing of record, individual memo, or other form that effectively records the purging.

51.1.6 Utilization of Intelligence Personnel

Information submitted will be analyzed for relationships with other intelligence data and when relationships are shown, the proper law enforcement officer/agency will be advised of the information. Information is gathered through a wide variety of means including:

A. Law Enforcement

1. Hattiesburg Police Department
2. Local agencies
3. State agencies
4. Federal agencies

B. Records

1. Law Enforcement
2. Other Criminal Justice agencies
3. County Courthouses
4. Banks
5. Business records
6. Schools
7. Military
8. Informants
9. Concerned Citizens
10. Surveillance
11. Media

51.1.7 Dissemination and Security of Criminal Intelligence Information

A. Information shall be disseminated only to law enforcement officers/agencies on a "need-to-know" or "right to know" basis.

1. Need to know – Requested information is pertinent and necessary to requestor in initiating, furthering or completing an investigation.

2. Right to know – Requestor has official capacity and statutory authority to the information being sought.

B Charts, graphs, memorandums, or any other relevant material shall be used to show trends, patterns, or relationships when practical.

C. All information going into the intelligence files shall be channeled through the appropriate intelligence file manager.

D The intelligence file manager will be responsible for the security of intelligence files to insure inadvertent disclosure of information does not occur. These files and their contents will be separately maintained and secured.

E. All intelligence records will be updated whenever new information on an existing file(s) or subject(s) is submitted.

F. Disseminated information may have security conditions or restrictions associated with the information. The security level may or may not be indicated on the documents if not indicated then the level of security will be determined by the method of dissemination and as described below. The security level may also be stated orally at the time or delivery such as person to person or during unit or taskforce briefing.

1. Unclassified

   All material disseminated form intelligence files in a bulk or accessible form such as e-mails, memorandums, or other broad dissemination is considered unclassified. This material is considered for department use only and is shared internally only to assist department personnel in the performance of their duty.

2. Restricted

   Restricted to law enforcement personnel having a specific need to know or right to know. This information may be issued to one person or may be restricted to a specific investigatory group or task force.

3. Confidential

   Information delivered directly to and intended for the recipients eyes only.

51.1.8 Legal and privacy issues

A. Public record generally includes any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics. Department incident reports, narratives, administrative reports, emails and the like are generally considered assessable by public records request.

B. It has been generally held that intelligence files are not subject to public record

inquiries. However, specific documents such as those mentioned above contained in the intelligence files are subject to release. In most cases these documents are also stored in standard department records files and will be released from those files.

C. The department will review any subpoena issued for intelligence files and determine whether or not it will be referred to the city attorney to be contested. Once a judge makes the determination as to what information will be released the department is obligated to follow that order. File managers will need to monitor the content and privacy concerns of the files under their control as all information (public and intelligence) is subject to subpoena.

D. True identity of the source should be used unless there is a need to protect the source. Whether or not confidential source identification is warranted, reports should reflect the name of the agency and the reporting individual. In those cases when identifying the source by name is not practical for internal security reasons, a code number may be used. A confidential listing of coded sources of information can then be retained by the intelligence file manager. In addition to indentifying the source, it may be appropriate in a particular case to describe how the source obtained the information.

51.1.9 Training

Training will be provided by attendance in off-site schools and seminars, in-service, roll call or other opportunities.

51.1.10 Review

A review of procedures and processes related to the intelligence file system and function will be conducted annually