DIVISION OF LAW ENFORCEMENT

CRIMINAL INTELLIGENCE FILE GUIDELINES

APRIL 1978

EVELLE J. YOUNGER Attorney General

STATE OF CALIFORNIA
DEPARTMENT OF JUSTICE

CRIMINAL INTELLIGENCE FILE GUIDELINES

Department of Justice
Division of Law Enforcement
April 1978

TABLE OF CONTENTS

I.	Criminal Intelligence File Objective	1
II.	Criminal Intelligence File Defined	2
III.	File Content	3
IV.	File Criteria	4 - 6
V.	Information Evaluation	7 - 8
VI.	Information Classification	9 - 10
VII.	Information Source	11
VIII.	Information Quality Control	12
IX.	File Dissemination	13
X.	File Purge	14 - 15
XI.	File Security	16
	Glossary	17 - 18
	Sample File Control Form	19

I. CRIMINAL INTELLIGENCE FILE OBJECTIVE

To provide the law enforcement agency with a sound data base which legitimately meets the needs of the agency in carrying out its efforts to protect the public and suppress criminal operations.

II. CRIMINAL INTELLIGENCE FILE DEFINED

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

A. Individuals who:

1. Are currently involved in or suspected of being involved in the planning, organizing, financing or commission of criminal activities; or who are suspected of having threatened, attempted, planned or performed criminal acts, or

2. Have an established association with known or suspected crime figures.

B. Organizations and businesses which:

1. 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

2. Are operated, controlled, financed, infiltrated or illegally used by crime figures.

III. FILE CONTENT

Material stored in the criminal intelligence file should be restricted to documents of criminal intelligence, and related information from public record* and media sources. Criminal History Record Information (CHRI)*, and information not meeting the agency's criteria for file input should be excluded from storage in the criminal intelligence file. Examples of excluded material are religious, political, or sexual information which does not relate to criminal conduct and associations with individuals which may not be of a criminal nature.

It is recommended that public record information [other than that which is excluded from disclosure by Government Code Section 6254(f) as limited by Section 1798 et. seq. of the Civil Code] and media information be retained in file systems separate from criminal intelligence. Although documents of criminal intelligence are public records, Government Code Section 6254(f) as limited by Section 1798 et. seq. of the Civil Code excludes them from disclosure. Separation of criminal intelligence from other files better protects both the confidentiality of the intelligence file and the individual's right of privacy.

In order to protect the confidentiality of the criminal intelligence file, it is also essential that Criminal History Record Information be excluded from the file. Criminal History Record Information is subject to specific audit and dissemination restrictions designed to protect the individual's right of privacy. Criminal History Record Information is easily obtainable from other law enforcement sources, thus, it is unnecessary to retain such information in intelligence files.**

---

*See Glossary for definition
**See Note under CHRI in Glossary

IV. FILE CRITERIA

All information to be retained in the criminal intelligence file should meet file criteria designed by the agency. These criteria should outline the parameters of the agency's criminal interests (crime categories) and provide specifics for determining whether subjects involved in these crime categories are suitable for file inclusion.

File input criteria will vary somewhat among agencies because of differences in size, functions, staffing, geographical location and crime problems. The following file input criteria are suggested as a model for a criminal intelligence file system. The categories listed in the model are not exhaustive and will vary according to the needs of the individual agency.

A. Permanent File

Information pertaining to an identifiable subject which meets the file criteria established by the agency is justified for retention in a permanent criminal intelligence file.

1. Information which relates that an individual, organization, business or gang has been involved, is involved or suspected of being involved in one or more of the following criminal activities:

   °Narcotic trafficking
   °Unlawful gambling
   °Loan sharking
   °Extortion
   °Vice and pornography
   °Infiltration of legitimate business for illegitimate purposes
   °Stolen securities
   °Bribery
   °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.
   °Threats to public officials and private citizens

2. In addition to falling within the confines of one or more of the above criminal activities, the subject to be entered into the permanent file should be

identifiable--distinguished by a unique identifying characteristic, e.g., date of birth, criminal identification number, driver's license number. Identification at the time of file input is necessary to distinguish the subject from any similars in file or any others that may be entered at a later time.

B. Temporary File:

Information which initially does not meet the criteria for permanent file storage but yet may have enough potential validity for the agency to want to retain it should be kept in a "Temporary" file. It is recommended that retention of information in a temporary file not exceed a one-year period unless compelling reason exists to extend this time period. During this period efforts should be made to identify the subject or validate the information so that 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 should be removed and destroyed. An individual, organization, business or gang may be given temporary file status in the following cases:

1. Subject is unidentifiable--subject, although suspected to be engaged in criminal activities, 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.

   °Possible criminal association--individual or organization, although not currently reported to be criminally active, associates with a known criminal and appears to be aiding or abetting illegal activities.

   °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.

3. Reliability/validity unknown--the reliability of the information source and/or the validity of the information content cannot be determined at the time of receipt; however, the information appears to be significant and merits temporary storage while verification attempts are made.

V. INFORMATION EVALUATION

Information retained in the criminal intelligence file should be evaluated for source reliability and content validity prior to filing.

The bulk of the data an intelligence unit receives consists of allegations or information which is initially unverified. Evaluating the information's source and content at the time of receipt indicates to future users the information's worth and usefulness and is essential in protecting the individual's right of privacy. Circulating information which may not have been evaluated or where the source reliability is poor or the content validity is doubtful is detrimental to the agency's operations and contrary to the individual's right of privacy.

To insure uniformity within the intelligence community, it is strongly recommended that stored information be evaluated according to the schedule set forth below.

Source Reliability:	Content Validity:
(A) Reliable	(1) Confirmed
(B) Usually Reliable	(2) Probable
(C) Unreliable	(3) Doubtful
(D) Unknown	(4) Cannot be Judged

Source Reliability

(A) Reliable	The reliability of the source is unquestioned or has been well tested in the past.
(B) Usually Reliable	The reliability of the source can usually be relied upon as factual. The majority of information provided in the past has proved to be reliable.
(C) Unreliable	The reliability of the source has been sporadic in the past.
(D) Unknown	The reliability of the source cannot be judged. Its authenticity or 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.

VI. INFORMATION CLASSIFICATION

Information retained in the criminal intelligence file should be classified to indicate the degree to which it should be kept confidential in order to protect sources, investigations, and the individual's right of privacy.

Classification also dictates the internal approval process which must be completed prior to dissemination of the information to personnel outside the agency. Classification of information should be the responsibility of a carefully selected and specifically designated individual in the intelligence unit.

The status of criminal intelligence is subject to continual change. It is important that information be reclassified to the appropriate security level as its sensitivity increases or decreases.

Classification systems may differ among agencies as to number of levels of security and levels of release authorization. In establishing a classification system, agencies should define types of information falling under each level of security and level of authority required for dissemination approval.

In order to insure conformity within the intelligence community, it is recommended that stored information be classified according to a system similar to that set forth below.

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.*	Intelligence Unit Commander
Class II - Sensitive	Restricted to law enforcement intelligence personnel having a specific need-to-know* and right-to-know.*	Intelligence Unit Supervisor
Class III - Restricted	Restricted to law enforcement personnel having a specific need-to-know* and right-to-know.*	Intelligence Unit Personnel

*Defined on page 13, section IX

Examples of classified information:

Class I - Confidential

1. Information pertaining to law enforcement cases currently under investigation.

2. Corruption (police or other government officials).

3. Informant identification information.

Class II - Sensitive

1. Criminal intelligence reports that refer to organized crime or terrorism.

2. Publications obtained through intelligence unit channels that are not deemed to be confidential.

Class III - Restricted

1. Reports that at an earlier date were classified confidential or sensitive and the need for high security no longer exists.

2. Non-sensitive reports published by local law enforcement agencies.

VII. INFORMATION SOURCE

In a number of situations, agencies may elect to identify information sources for items stored in their criminal intelligence files. Accordingly, each law enforcement agency should establish criteria which would indicate when source identification would be appropriate.

The value of information stored in a criminal intelligence file is often directly related to the source of such information. Some factors to consider in determining whether source identification is warranted include:

- The nature of the information reported.
- The potential need to refer to the source's identity for further investigative or prosecutorial activity.
- The reliability of the source.

Where source identification is warranted, it should reflect the name of the agency and the individual providing the information. In those cases where identifying the source by name is not practical for internal security reasons, a code number could be used. A listing of coded sources of information can then be retained by the intelligence 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 _____ Police Department saw" a particular event at a particular time.

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

VIII. INFORMATION QUALITY CONTROL

Information to be stored in the criminal intelligence file should undergo a review for compliance with established file input guidelines and agency policy prior to being filed.

This quality control requirement should be the responsibility of a carefully selected and specifically designated individual in the intelligence unit.

The quality control reviewer is responsible for seeing that all information entered into the criminal intelligence file conforms with the agency's file criteria and has been properly evaluated and classified. Review of file input will assure the agency of the quality of its criminal intelligence file in meeting established guidelines.

IX. FILE DISSEMINATION

In order to protect the right of privacy of individuals contained in the criminal intelligence file and to maintain the confidentiality of the sources and the file itself, agencies should adopt sound procedures for disseminating stored information.

Section 703B of the California Administrative Code, Chapter I, Title 11 limits dissemination of criminal history record information to criminal justice agencies and only to those with a specific need-to-know as well as a right-to-know. These terms which can be applied to intelligence information access are defined as follows:

> Need-to-know--Requested information is pertinent and necessary to the requester agency in initiating, furthering, or completing an investigation.
>
> Right-to-know--Requester agency has official capacity and statutory authority to the information being requested.

The classification and evaluation assigned the information are, in part, dissemination controls. They denote who may receive the information as well as the internal approval level(s) required for release of the information.

The integrity of the criminal intelligence file can be maintained only by strict adherence to proper dissemination guidelines. Abuses in the operation of the system due to failure to comply with dissemination guidelines may result in the violation of an individual's right of privacy and endanger the confidentiality of the file itself.

To eliminate unauthorized use and abuses of the system, a department may wish to utilize a dissemination control form which could be maintained with each stored document. This control form could record the date of the request, the name of the agency and individual requesting the information, the need-to-know, the information provided and the name of the employee handling the request. An example of the form is attached.

Depending upon the needs of the agency, the control form may be designed to also record other items useful to the agency in the management of its operations.

X. FILE PURGE

Information stored in the criminal intelligence file should be periodically reviewed and purged to insure that the file is current, accurate and relevant to the needs and objectives of the agency and to safeguard the individual's right of privacy as guaranteed under federal and state laws.

Law enforcement agencies have an obligation to keep stored information on individuals current and accurate. Reviewing of criminal intelligence should be done on a continual basis as agency personnel use the material in carrying out day-to-day activities. In this manner, information which appears to be no longer useful or cannot be validated can be immediately purged from the file and destroyed.

To insure that the review and purge of the file are done systematically, agencies should develop purge criteria and time schedules. Operational procedures of the purge as well as the manner of destruction for purged materials should be established.

A. Purge Criteria

General considerations which may be applied to the reviewing and purging of information stored in the criminal intelligence file are as follows:

1. Utility

°How often is the information used?
°For what purpose is the information being used?
°Who uses the information?

2. Timeliness and Appropriateness

°Is the information outdated?
°Is the information relevant to the needs and objectives of the agency?
°Is the information relevant to the purpose for which it was collected and stored?
°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?

3. Accuracy and Completeness

°Is the information still valid?
°Is the information adequate for identification purposes?
°Can the validity of the data be determined through investigative techniques?

B. Purge Time Schedule

Review of the criminal intelligence file for purging purposes can vary from once each year to once every seven years. Local agencies should develop a schedule best suited to their needs.

C. Manner of Destruction

Material purged from the criminal intelligence file should be destroyed under the supervision of members of the intelligence unit and in accordance with applicable state and local regulations.

XI. FILE SECURITY

The criminal intelligence file should be located in a secured area with file access restricted to authorized personnel.

Physical security of the criminal intelligence file is imperative to maintain the confidentiality of the information stored in the file and to ensure the protection of the individual's right of privacy.

GLOSSARY

Criminal History Record Information (CHRI)

> "Criminal history record information" means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations, or other formal criminal charges, and any disposition arising therefrom, sentencing, correctional supervision, and release. The term does not include identification information such as fingerprint records to the extent that such information does not indicate involvement of the individual in the criminal justice system. Section 20.3b, Title 28, Chapter 1, Part 20, Code of Federal Regulations.

Note: The term criminal history record information is not limited to what criminal justice agencies commonly call rap sheets. Whenever personal identifiers, such as name and address, exist on the same piece of paper with one of the formal transactions of the criminal justice system, CHRI is created. For example, a fingerprint card which shows that an individual has been arrested is CHRI; take away the reference to the arrest and it is not CHRI.

Clearly, CHRI will appear in many places: police blotters, court dockets, arrest reports, pre-sentence investigations, wanted posters. Every time CHRI appears, it is governed by Title 28, unless specifically exempted. There are six exemptions to Title 28:[1]

> The regulations in this subpart [b] shall not apply to criminal history information contained in: (1) poster, announcements, or lists for identifying or apprehending fugitives or wanted persons; (2) original records of entry such as police blotters maintained by criminal justice agencies, compiled chronologically and required by law or long standing custom to be made public, if such records are organized on a chronological basis; (3) court records of public judicial proceedings; (4) published court or administrative opinions or public judicial, administrative or legislative proceedings; (5) records of traffic offenses maintained by State departments of transportation, motor vehicles or the equivalent thereof for the purpose of regulating the issuance, suspension, revocation, or renewal of driver's, pilot's or other operators' license; (6) announcements of executive clemency. Section 20.20b.

[1] How to Implement Privacy and Security, Theorum Handbook

Criminal Intelligence

> Information which has been processed--collected, evaluated, collated, analyzed--into data useful for law enforcement investigative purposes. Intelligence involves data collection from both overt and covert sources and is not necessarily directed at a specific arrest or prosecution.

Public Record

> "Public record" 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. (Chapter 3.5, Section 6252(d), California State Government Code.)

For purposes of these guidelines, public record information includes only that information to which the general public normally has direct access, i.e., birth or death certificates, county recorder's information, incorporation information, etc. It does not include those types of information excluded from disclosure by Government Code Section 6254(f), namely:

> Records of complaints to or investigations conducted by, or records of intelligence information or security procedures of, the Office of the Attorney General and the Department of Justice, and any state or local police agency, or any such investigatory or security files compiled by any other state or local agency for correctional, law enforcement or licensing purposes.

FILE CONTROL #

	DATE	AGENCY / INDIVIDUAL	PURPOSE	INFORMATION	(PAGE OR)	PERSON H... FOR...
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						

END