CRIMINAL INTELLIGENCE FILE GUIDELINES

Prepared by LEIU

An International Law Enforcement Intelligence Network
"Founded in 1956"

Revised: November 3, 2008

ASSOCIATION OF
LAW ENFORCEMENT INTELLIGENCE UNITS

Your Voice at the National Level!

FOREWORD

These guidelines are provided to member agencies as an ongoing effort by your Executive Board to promote professionalism, provide protection for citizens' privacy, and yet enable law enforcement agencies to collect information in their pursuit of organized crime entities. It has long been established that agencies engaged in the collection, storage, analysis, and dissemination of criminal intelligence information must operate under specified guidelines to ensure abuses to this process do not occur. Along with operational guidelines, it is essential that member agencies adopt file procedures as a check and balance against inappropriate activities.

Each member agency is encouraged to have a written policy regarding its file procedures. A member may wish to adopt these guidelines or modify them to meet its particular state or local policies, laws, or ordinances. Member agencies with existing written file policies are commended and are encouraged to examine this document for any ideas that may augment their guidelines.

L.E.I.U. and its member agencies are in the forefront in promoting the value of the criminal intelligence function as a tool on combating organized crime and terrorism. Please do not hesitate to contact members of your Executive Board if you have questions, wish to discuss new ideas, or have suggestions for training.

Sincerely,

Russell M. Porter

General Chairperson
Association of Law Enforcement Intelligence Units

CRIMINAL INTELLIGENCE FILE GUIDELINES

I. CRIMINAL INTELLIGENCE FILE GUIDELINES

These guidelines were established to provide the law enforcement agency with an information base that meets the needs of the agency in carrying out its efforts to protect the public and suppress criminal operations. These standards are designed to bring about an equitable balance between the civil rights and liberties of citizens and the needs of law enforcement to collect and disseminate criminal intelligence on the conduct of persons and groups who may be engaged in systematic criminal activity.

II. CRIMINAL INTELLIGENCE FILE DEFINED

A criminal intelligence file consists of stored information on the activities and associations of:

A. Individuals who:

1. Are suspected of being involved in the actual or attempted planning, organizing, financing, or commission of criminal acts; or

2. Are suspected of being involved in criminal activities with known or suspected crime figures.

B. Organizations, businesses, and groups that:

1. Are suspected of being involved in the actual or attempted planning, organizing, financing, or commission of criminal acts; or

2. Are suspected of being operated, controlled, financed, or infiltrated by known or suspected crime figures for use in an illegal manner.

III. FILE CONTENT

Only information with a criminal predicate and which meets the agency's criteria for file input should be stored in the criminal intelligence file. Specifically excluded material includes:

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

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

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

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

E. Criminal Offender Record Information (CORI) should be excluded from an intelligence file. This is because CORI may be subject to specific audit and dissemination restrictions which are designed to protect an individual's right to privacy and to ensure accuracy.

F. Also excluded are associations with individuals that are not of a criminal nature.

State law or local regulations may dictate whether or not public record and intelligence information should be kept in separate files or commingled. Some agencies believe that separating their files will prevent the release of intelligence information in the event a subpoena is issued. This belief is unfounded, as all information requested in the subpoena (both public and intelligence) must be turned over to the court. The judge then makes the determination on what information will be released.

The decision to commingle or separate public and intelligence documents is strictly a management decision. In determining this policy, administrators should consider the following:

A. Records relating to the conduct of the public's business that are prepared by a state or local agency, regardless of physical form or characteristics, may be considered public and the public has access to these records.

B. Specific types of records (including intelligence information) may be exempt from public disclosure.

C. Regardless of whether public record information is separated from or commingled with intelligence data, the public may have access to public records.

D. The separation of public information from criminal intelligence information may better protect the confidentiality of the criminal file. If a request is made for public records, an agency can release the public file and leave the intelligence file intact (thus less apt to accidentally disclose intelligence information).

E. Separating of files is the best theoretical approach to maintaining files; however, it is not easy to do. Most intelligence reports either reference public record information or else contains a combination of intelligence and public record data. Thus, it is difficult to isolate them from each other. Maintaining separate public and intelligence files also increases the amount of effort required to index, store, and retrieve information.

IV. FILE CRITERIA

All information retained in the criminal intelligence file should meet file criteria prescribed by the agency. These criteria should outline the agency's crime categories and provide specifics for determining whether subjects involved in these crimes are suitable for file inclusion.

File input criteria will vary among agencies because of differences in size, functions, resources, geographical location, crime problems, etc. The categories listed in the suggested model below are not exhaustive.

A. Permanent Status

1. Information that relates an individual, organization, business, or group is suspected of being involved in the actual or attempted planning, organizing, financing, or committing of one or more of the following criminal acts:

   - Narcotic trafficking/manufacturing
   - Unlawful gambling
   - Loan sharking
   - Extortion
   - Vice and pornography
   - Infiltration of legitimate business for illegitimate purposes
   - Stolen securities

- Bribery
- Major crime including homicide, sexual assault, burglary, auto theft, kidnapping, destruction of property, robbery, fraud, fencing stolen property, and arson
- Manufacture, us of, 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 above criminal activities, the subject/entity to be given permanent status must be identifiable--distinguished by a name and unique identifying characteristics (e.g., date of birth, criminal identification number, driver's license number, address). Identification at the time of file input is necessary to distinguish the subject/entity from existing file entries and those that may be entered at a later time. NOTE: The exception to this rule involves modus operandi (MO) files. MO files describe a unique method of operation for a specific type of crime (homicide, fraud) and may not be immediately linked to an identifiable suspect. MO files may be retained indefinitely while additional identifiers are sought.

B. Temporary Status:

Information that does not meet the criteria for permanent storage but may be pertinent to an investigation involving one of the categories previously listed should be given "temporary" status. It is recommended the retention of temporary information not exceed one year unless a compelling reason exists to extend this time period. (An example of a compelling reason is if several pieces of information indicate that a crime has been committed, but more than a year is needed to identify a suspect.) During this period, efforts should be made to identify the subject/entity or validate the information so that its final status may be determined. If the information is still classified temporary at the end of the one-year period, and a compelling reason for its retention is not evident, the information should be purged. An individual, organization, business, or group may be given temporary status in the following cases:

1. **Subject/entity is unidentifiable** - subject/entity (although suspected of being engaged in criminal activities) has no known physical descriptors, identification numbers, or distinguishing characteristics available.

2. **Involvement is questionable** - involvement in criminal activities is suspected by a subject/entity which has either:
   - **Possible criminal associations** - individual, organization, business, or group (not currently reported to be criminally active) associates with a known criminal and appears to be jointly involved in illegal activities.

   - **Criminal history** - individual, organization, business, or group (not currently reported to be criminally active) that has a history of criminal conduct, and the circumstances currently being reported (i.e., new position or ownership in a business) indicates they may again become criminally active.

3. **Reliability/validity unknown** - the reliability of the information sources 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 verification attempts are made.

V. INFORMATION EVALUATION

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

The bulk of the data an intelligence unit receives consists of unverified allegations or information. Evaluating the information's source and content indicates to future users the information's worth and usefulness. Circulating information which may not have been evaluated, 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 to privacy.

To ensure uniformity with the intelligence community, it is strongly recommended that stored information be evaluated according to the criteria set forth below.

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 proven 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 by an investigator or another independent, reliable source.

(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 judged. Its authenticity has not yet been determined by either experience or investigation.

VI. INFORMATION CLASSIFICATION

Information retained in the criminal intelligence file should be classified in order to protect sources, investigations, and the individual's right to privacy. Classification also indicates the internal approval which must be completed prior to the release of the information to persons outside the agency. However, the classification of information in itself is not a defense against a subpoena duces tecum.

The classification of criminal intelligence information is subject to continual change. The passage of time, the conclusion of investigations, and other factors may affect the security classification assigned to particular documents. Documents within the intelligence files should be reviewed on an ongoing basis to ascertain whether a higher or lesser degree of document security is required to ensure that information is released only when and if appropriate.

Classification systems may differ among agencies as to the number of levels of security and release authority. In establishing a classification system, agencies should define the types of information for each

security level, dissemination criteria, and release authority. The system listed below classifies data maintained in the Criminal Intelligence File according to one of the following categories:

Sensitive

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

2. Corruption (police or other government officials), or other sensitive information.

3. Informant identification information.

4. Criminal intelligence reports which require strict dissemination and release criteria.

Confidential

1. Criminal intelligence reports not designated as sensitive.

2. Information obtained through intelligence unit channels that is not classified as sensitive and is for law enforcement use only.

Restricted

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

2. Non-confidential information prepared for/by law enforcement agencies.

Unclassified

1. Civic-related information to which, in its original form, the general public had direct access (i.e., public record data).

2. News media information - newspaper, magazine, and periodical clippings dealing with specified criminal categories.

VII. INFORMATION SOURCE

In all cases, source identification should be available in some form. The true identify of the source should be used unless there is a need to protect the source. Accordingly, each law enforcement agency should establish criteria that 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 or prosecutorial activity.

- The reliability of 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 unit commander. In addition to identifying the source, it may be appropriate in a particular case to describe how the source obtained the information (for example "S-60, a reliable police informant heard" or "a reliable law enforcement source of the police department saw" a particular event at a particular time).

VIII. INFORMATION QUALITY CONTROL

Information to be stored in the criminal intelligence file should undergo a thorough review for compliance with established file input guidelines and agency policy prior to being filed. The quality control reviewer is responsible for seeing that all information entered into the criminal intelligence files conforms with the agency's file criteria and has been properly evaluated and classified.

IX. FILE DISSEMINATION

Agencies should adopt sound procedures for disseminating stored information. These procedures will protect the individual's right to privacy as well as maintain the confidentiality of the sources and the file itself.

Information from a criminal intelligence report can only be released to an individual who has demonstrated both a "need-to-know" and a "right-to-know."

"**Right-to-know"** Requestor has official capacity and statutory authority to the information being sought.

"Need-to-know" Requested information is pertinent and necessary to the requestor agency in initiating, furthering, or completing an investigation.

No "original document" which has been obtained from an outside agency is to be released to a third agency. Should such a request be received, the requesting agency will be referred to the submitting agency for further assistance.

Information classification and evaluation 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. In order to encourage conformity within the intelligence community, it is recommended that stored information be classified according to a system similar to the following.

Security Level	Dissemination Criteria	Release Authority
Sensitive	Restricted to law enforcement personnel having a specific need-to-know and right-to-know	Intelligence Unit Commander
Confidential	Same as for sensitive	Intelligence Unit Manager or designee
Restricted	Same as for Sensitive	Intelligence Unit Supervisor or designee
Unclassified	Not restricted Personnel	Intelligence Unit

The integrity of the criminal intelligence file can be maintained only by strict adherence to proper dissemination guidelines. To eliminate unauthorized use and abuses of the system, a department should utilize a dissemination control form that could be maintained with each stored document. This control form would 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. Depending upon the needs of the agency, the control form also may be designed to record other items useful to the agency in the management of its operations. This control form also may be subject to discovery.

X. FILE REVIEW AND PURGE

Information stored in the criminal intelligence file should be reviewed periodically for reclassification or purge in order to: ensure that the file is current, accurate, and relevant to the needs and objective of the agency; safeguard the individual's right of privacy as guaranteed under federal and state laws; and, ensure that the security classification level remains appropriate.

Law enforcement agencies have an obligation to keep stored information on subjects 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 that is no longer useful or that cannot be validated can immediately be purged or reclassified where necessary.

To ensure that all files are reviewed and purged systematically, agencies should develop purge criteria and schedules. Operational procedures for the purge and the method of destruction for purged materials should be established.

A. Purge Criteria:

General considerations for 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 this investigation still ongoing?
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?

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. Review and Purge Time Schedule:

Reclassifying and purging information in the intelligence file should be done on an ongoing basis as documents are reviewed. In addition, a complete review of the criminal intelligence file for

purging purposes should be undertaken periodically. This review and purge schedule can vary from once each year for documents with temporary status to once every five years for permanent documents. Agencies should develop a schedule best suited to their needs and should contact their legal counsel for guidance.

C. Manner of Destruction:

Material purged from the criminal intelligence file should be destroyed. Disposal is used for all records or papers that identify a person by name. It is the responsibility of each agency to determine that their obsolete records are destroyed in accordance with applicable laws, rules, and state or local policy.

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 to privacy.

Glossary

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.

"Member of the public" means any person, except a member, agent, officer, or employee of a federal, state, or local agency acting within the scop of his or her membership in an agency, office, or employment.

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.)

CRIMINAL OFFENDER RECORD INFORMATION (CORI)

CORI is defined as summary information to arrests, pretrial proceedings, sentencing information, incarcerations, parole and probation.

a. Summary criminal history records are commonly referred to as "rap sheets." Data submitted on fingerprint cards, disposition of arrest and citation forms and probation flash notices create the entries on the rap sheet.