California Department of Justice Division of Law Enforcement Bureau of Investigation and Intelligence

California
Attorney General's

Model Standards and Procedures for

Maintaining Criminal Intelligence Files

and

Criminal Intelligence Operational Activities

Revised
November 2007

California
Attorney General's

Model Standards and Procedures for

Maintaining Criminal Intelligence Files

and

Criminal Intelligence Operational Activities

Revised by:
Harry Joseph Colombo and Robert C. Nash
Deputy Attorneys General
Appeals, Writs and Trials Unit
Division of Criminal Law

Revised
November 2007

Table of Contents

Section One

Criminal Intelligence Files

I. Introduction 1

II. Criminal Intelligence File Objective 2

III. Definition of Terms 2

IV. Establishing the Intelligence Function 5

V. Criminal Intelligence Files 5

VI. File Content 14

VII. Analysis 17

VIII. Information Dissemination 17

IX. Maintenance of the File 20

X. Review and Purge Procedures 22

XI. Closing Comments 25

Section Two

Criminal Intelligence Operational Activities

I. Authorized Intelligence Operational Activities 29

II. Use of Undercover Criminal Intelligence Officers 31

III. Additional Limitations on Undercover Criminal Intelligence Officers 36

IV. Standards and Responsibilities of Commanders of Criminal Intelligence Sections 37

V. Auditing and Oversight 38

VI. Closing Comments 39

Appendix A 40

Appendix B 46

Section One

Criminal Intelligence Files

I. Introduction

The operation of an intelligence system requires an agency to understand and respect the legal concepts that combine to make up the "right of privacy." The Standards and Procedures set forth below recognize and abide by the policies and guidelines expressed in Title 28, Code of Federal Regulations, Part 23 (hereafter 28 CFR 23).[1] These Standards and Procedures acknowledge the legitimate needs of law enforcement to carry out criminal intelligence assignments within the limits created by California and federal constitutional and statutory protections, including the guaranteed rights: (1) of privacy, (2) to receive, hold and express ideas, (3) to dissent freely, (4) to write and to publish, (5) to petition for the redress of grievances, and (6) to associate publicly and privately for any lawful purpose.

The *National Criminal Intelligence Sharing Plan* recommends adoption of ". . . at a minimum, the standards required by . . . 28 CFR 23, regardless of whether or not an intelligence system is federally funded." (See Executive Summary, p. IX.) Thus, it is strongly recommended that all systems in California adopt 28 CFR 23 as a "minimum" guideline. Moreover, the California Department of Justice advocates adoption of these Standards and Procedures, which are in certain respects more restrictive than 28 CFR 23.

"Intelligence" is the gathering, analysis, storage/maintenance, and sharing of information about persons and organizations in support of legitimate policy objectives. In the case of criminal intelligence, the policy objective is to promote greater public safety. Both the acquisition and dissemination of this information involves "the right of privacy" articulated by the United States Supreme Court in *Griswold v. Connecticut* (1965) 381 U.S. 479, and Article I, section 1 of the California Constitution.[2]

"Privacy" at the federal level is not an express constitutional right. It is an "implied constitutional right" as expressed by the five-justice majority in *Griswold*.[3] This implied right is applicable to the states as part of the Fourteenth Amendment's due process requirement. (*Griswold v. Connecticut, supra*, 381 U.S. at pp. 481-482.)[4]

1. See Appendix A for the full text.

2. This section provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." The phrase "and privacy" was added by an initiative adopted by the voters on November 7, 1972 (the Privacy Initiative).

3. Two of the remaining four justices agreed with the result but not the reasoning, and two disagreed with both the result and the reasoning.

4. Both of the dissenting opinions found that, while the Connecticut law at issue–prohibiting the use of "any drug, medicinal article or instrument for the purpose of preventing conception"–was offensive, it was not in violation of the United States Constitution.

On the other hand, the California Constitution ***expressly provides*** that privacy is an "inalienable right" of all Californians. The California Supreme Court has described informational privacy as the core value protected by our state constitutional right to privacy. (*Hill v. National Collegiate Athletic Assn.* (1994) 7 Cal.4th 1, 35, citing *White v. Davis* (1975) 13 Cal.3d 757, 774.) "'The constitutional provision is self-executing; hence it confers a judicial right of action on all Californians. . . . Privacy is protected not merely against state action; it is considered an inalienable right which may not be violated by anyone.'" (*Hill v. National Collegiate Athletic Assn., supra*, 7 Cal.4th at p. 18, citation omitted, quoting *Porten v. University of San Francisco* (1976) 64 Cal. App. 3d 825, 829.)

Put simply, obtaining intelligence involves invading privacy to the extent the law permits; maintaining this information in a way that protects the privacy of those who are the subjects of the intelligence file(s); and disseminating the intelligence only as the law permits, given the private nature of the information.

II. Criminal Intelligence File Objective

The objective of criminal intelligence files is to obtain, maintain and use information from legal, reliable sources that help law enforcement agencies in protecting the public and reducing crime while protecting appropriate privacy rights.

III. Definition of Terms

Analysis — This term refers to the process by which legally obtained data is evaluated by qualified personnel to determine whether it is useful intelligence.[5]

Analysts — Typically, these are non-sworn specialists employed by law enforcement or other governmental agencies concerned with public safety whose training enables them to engage in analysis of information for purposes of creating an intelligence file and validating existing intelligence files.[6]

Audit — The process of objective examination of the policies and procedures pertaining to the maintenance of intelligence files – as well as

5. There is no statutory definition of "analysis." Title 28 of the Code of Federal Regulations implies this definition in 28 CFR § 23.3(b)(3).

6. Title 28 of the Code of Federal Regulations contemplates the use of analysts in section 23.20, subdivision (c), where it refers to ". . . a trained . . . law enforcement or criminal investigative agency . . . employee . . . ."

examination of the files or a meaningful sample of the files to determine whether the intelligence system is in compliance with 28 CFR 23.

Criminal Intelligence File — A file that contains criminal intelligence information.

Criminal Intelligence Information — Information which has been evaluated to determine that it:

1. Is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity; and
2. Meets the submission criteria required by 28 CFR § 23.20(b).

Criminal Predicate — This term is the standard by which the determination as to whether information may be used to create an intelligence file is made. It means that there exists a "reasonable suspicion" based on the analysis of legally obtained information that the subject of the information is or may be involved in "definable criminal conduct and/or activity that supports, encourages, or otherwise aids definable criminal conduct."

Dissemination — The sharing of criminal intelligence among law enforcement authorities in any agency or agencies on a need to know, right to know basis with the assurance that cooperating authorities comply with 28 CFR § 23.20 or more stringent requirements.

Infiltration — Development of an ongoing relationship between an undercover officer and a target or non-target group or organization, by participating in and/or attending a target or non-target group or organization's activities, for the purpose of gathering criminal intelligence on the target group or organization.

Information — This term means data from "any legal source" that can be analyzed to determine if it provides intelligence.

Intelligence Systems — All aspects of the individual agency intelligence files and the inter-jurisdictional pooling of the information contained in the individual agency files.[7]

Maintenance — Criminal intelligence files subject to these guidelines shall be maintained as required by 28 CFR § 23.20(g), (h), (m) and (n).

Monitoring — The short term or preliminary act of observing or watching the activities of an individual or organization for the purposes of gathering information relevant to an Initial Lead Investigation. Continuous or

7. See 28 CFR §§ 23.20(n), 23.30(c), (d).

prolonged observation by clandestine means is not permitted during an Initial Lead Investigation.

Need to Know — This is the second part of the two-part test to determine whether dissemination ought to occur. A need to know is a state of facts that supports the legitimacy of access to specific intelligence by a person with a right to know. The need to know must be pertinent to and necessary to the performance of a specific law enforcement activity.

Non-target Group or Organization — A group or organization that is not the subject of an authorized criminal intelligence assignment, but there is a reasonable basis for believing that the presence of an undercover officer in the non-target group or organization will enable the undercover officer to infiltrate the target organization.

Operating Guidelines — The written guidelines created by each agency gathering, maintaining and disseminating intelligence that govern all aspects of the intelligence activity.[8]

Purge — The elimination–through destruction of the contents–of the intelligence file from the intelligence system when it no longer has validity.

Reasonable Suspicion — That state of known information which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise.[9]

Reliability — The process by which an information source is evaluated to determine the credibility that should be given to the information.[10]

Right to Know — This term is mentioned in 28 CFR § 23.20(e) and (g) but not directly defined by either subsection. Section 28.20(e) imposes the qualification that the right to know must be in ". . . the performance of a law enforcement activity . . . ." It is the status of being a person or entity engaged in law enforcement activity that, because of official capacity and/or statutory authority, may have access if there is a need to know.[11]

Target — A group, organization or individual that is the intended subject of an authorized criminal intelligence assignment because there is a reasonable suspicion that the group or organization is, or individual

8. See 28 CFR §§ 23.2, 23.20, and 23.30(c), (d).
9. See 28 CFR §§ 28.20(a); *United States v. Arvizu* (2002) 534 U.S. 266, 273-274, 277.
10. See generally 28 CFR § 23.20(g), (h).
11. See 28 CFR § 23.20(e), (g).

members of the group or organization are, involved in a definable criminal activity or enterprise.

Undercover Officer — A law enforcement officer who disguises or conceals his or her identity as a law enforcement officer for the purpose of gathering criminal intelligence through the development of ongoing relationships with individuals or organizations.

Validation — The ongoing process that ensures the information in the intelligence system is current and relevant to the criminal predicate(s) that supported its initial entry into the system or provides reasonable suspicion of additional criminal predicates.[12]

IV. Establishing the Intelligence Function

In order to carry out the criminal intelligence file objective (see II, supra), an agency needs to create written policies and procedures that govern the system. Such guidelines are required by 28 CFR 23 in order to safeguard individual rights. (See, e.g., 28 CFR § 23.20.)

Responsibility for the proper operation of an intelligence system is to be assumed at the highest levels of the law enforcement agency. (See 28 CFR § 23.30(c), (d).) The guidelines should be promulgated by the head of the agency and should clearly express his or her expectations as to every aspect of the intelligence operation.

Likely, many existing operations do not have such written guidelines in place or will not have reviewed the guidelines in many years. Time should be taken to either create or review guidelines so that policies and procedures are current and clear.

We recommend that the guidelines address the various topics discussed in the balance of this document. All guidelines should be reviewed and approved by the appropriate legal counsel to ensure compliance with any applicable local laws, codes or ordinances.

V. Criminal Intelligence Files

A. General Considerations

1. An intelligence file will consist of analyzed data from sources ranging from "open source" (books, newspapers, magazines, scientific or technical journals, internet, etc.) to "confidential" (such as informants and classified reports). The only limits 28 CFR 23 places on data that may be analyzed are:

12. See 28 CFR §§ 23.20(a), (c) and (h), 23.3(b)(6).

- It must be legally obtained (see 28 CFR § 23.20(d), (k)).
- It may not include information about "political, religious or social views, associations or activities" *unless* such information relates "directly to definable criminal conduct or activity and the subject of the information is reasonably suspected of involvement in that conduct or activity. (See 28 CFR § 23.20(b).)

2. 28 CFR § 23.20(b) also imposes a requirement that there be no use of an intelligence operation to interfere with or disrupt lawful political activities.

3. Once data has been lawfully collected, it goes through several steps that will terminate in one of the following three results:

   - Destruction of the data because there is no criminal predicate and no reasonable likelihood of developing a criminal predicate,
   - Determination that, although no criminal predicate then exists or no person or group has yet been linked to the predicate, there is a reasonable likelihood that within a reasonable period of time (DOJ uses one year) evidence of the predicate or identity of the person or group will be available,[13] or
   - Determination that a criminal predicate exists.

One further general comment must be made at this point. The federal Department of Justice has opined that so-called "non-criminal identifying information" may be included in an intelligence file as long as the information is clearly labeled as such. The California Department of Justice has rejected this policy and does not include such information in its intelligence files. *It is strongly recommended that such information not be included regardless whether it is properly labeled*. The reasoning is that there is substantial danger this category of information could be used to introduce information having no relevance to a criminal predicate but still identifying a person or organization into an intelligence file. Support for this view (we submit) is found in 28 CFR 23.20(a), which establishes the criminal predicate requirement and then states, ". . . and the information [which may be collected, maintained and disseminated] is relevant to that criminal conduct or activity [the criminal predicate]." Because non-criminal identifiers have

13. These files may be referred to by various names: working files, temporary files, and developmental files.

no relevance to the criminal predicate, it is the position of the California Department of Justice that the clear language of 28 CFR 23 prohibits their inclusion in a file.[14]

B. **Policies Governing Criminal Intelligence Files**

1. **Supervision of data entry** — All criminal intelligence data shall be reviewed by the commanding officer, Criminal Intelligence Section, prior to entry into any criminal intelligence file. The commanding officer shall determine that the criminal intelligence data conforms to these Standards and Procedures and was not obtained in violation of any applicable Federal, State, or local law, policy or ordinance. Criminal intelligence information will not be placed in any criminal intelligence file unless approved by the commanding officer. The badge number of the commanding officer will become part of the file.

2. **Information submission criteria**

   a. The Criminal Intelligence Section shall only collect[15] or maintain criminal intelligence information concerning an individual or organization if there is reasonable suspicion that the individual or organization is involved in criminal conduct or activity, as set forth below in subsection B.4.a., and the information is relevant to the criminal conduct or activity. The existence of the reasonable suspicion will be based on specific, articulable facts that will be documented in the criminal intelligence file.

   b. In addition to collecting and maintaining criminal intelligence information as set forth above in subsection B.2.a., the Criminal Intelligence Section may also collect or maintain information concerning an individual or organization if the information satisfies the temporary file criteria set forth below in subsection B.4.b. Information may be entered into temporary files when a determination has been made that, although the reasonable suspicion standard for an individual and/or organization has not been met, there is a reasonable likelihood that within one year the standard

14. If a system decides to follow the federal approach, an option–preferable to simply including the information in the general file with the necessary label–exists. The option is to have a discrete file section within the specific file labeled "location/identification date" with respect to a specific person, group or organization.

15. As used in these Standards and Procedures, the terms "collect" or "collecting" refer to the gathering and/or maintaining of information for criminal intelligence files or temporary files. These terms do not refer to monitoring when no information is collected.

for entry into the criminal intelligence file system will be available.

c. The Criminal Intelligence Section shall not collect or maintain information about the political, religious, social views, associations or activities of any individuals or any group, association, corporation, business, partnership , or other organization, unless such information directly relates to criminal conduct or activity and there is a reasonable suspicion that the subject of the information is or may be involved in that criminal conduct or activity.

3. **Excluded material** — Only lawfully collected information, based on a reasonable suspicion of criminal activity, that meets these Standards and Procedures, as well as any other relevant policies from the local law enforcement agency regarding criteria for file input, should be stored in criminal intelligence files. Information that shall be specifically excluded from criminal intelligence files 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 race, gender, age, or ethnic background.

   c. Information on an individual or group merely on the basis of religious or political affiliations or beliefs.

   d. Information on an individual or group merely on the basis of personal habits and/or predilections that do not violate any criminal laws or threaten the safety of others.

   e. Information on an individual or group merely on the basis of involvement in expressive activity that takes the form of non-violent civil disobedience that amounts, at most, to a misdemeanor offense.

4. **File criteria** — There are two types of intelligence records: criminal intelligence files; and temporary files.

   a. **Criminal intelligence files** — Information may be retained in the criminal intelligence files for up to five (5) years. At that time, criminal information will be automatically purged *unless* new criminal intelligence has been developed establishing a reasonable suspicion that the individual and/or organization continues to be involved in a definable criminal activity or enterprise. When updated criminal

intelligence is added into the criminal intelligence files on a suspect individual or organization already listed in the database, such entries reset the five-year standard for retention of that file. Criminal intelligence files will be periodically reviewed for compliance with this policy consistent with the purging requirements contained in Section X.

b. **Temporary files** — Information may be entered into temporary files when a determination has been made that, although the reasonable suspicion standard for an individual and/or organization has not been met, there is a reasonable likelihood that *within one year* the standard for entry into the criminal intelligence file system may be available. Temporary files shall not be retained for longer than one year. At the end of one year, temporary files must be either purged or converted into criminal intelligence files, if the information satisfies the criteria for submission into criminal intelligence files. All temporary files shall be specifically designated as such, and they will be kept distinctly separate from the criminal intelligence files.

1) Security for temporary files — All of the specific security requirements for criminal intelligence files, described below in subsection IX.B., shall also be followed for temporary files.

2) Information dissemination from temporary files — All of the specific requirements on dissemination of information from criminal intelligence files, described below in subsection VIII.A.1.-6., shall also be followed for temporary files.

3) Supervision of data entry into temporary files — The commanding officer of the Criminal Intelligence Section shall periodically review temporary files to determine that these Standards and Procedures are followed, and that the information contained in the temporary files was not obtained in violation of any applicable Federal, State, or local law or ordinance, or local police department policies.

5. **Information classification**

A criminal intelligence file will only be useful if its information is reliable, accurate and current. As discussed more fully, *infra*, there are two critical components in information that are

the determinants of these values. These are: (1) the reliability of the source, and (2) the validity of the content.

- Information to be retained in files pursuant to these Standards and Procedures shall be labeled for source reliability and content validity prior to entry or submission. Circulating information that has not been evaluated, where the source reliability is poor or the content validity is doubtful, is detrimental to a local police department's criminal intelligence operations and is contrary to the individual's right to privacy.
- 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 or dissemination criteria assigned to particular documents.
- Documents within the intelligence files should be reviewed on an ongoing basis to ascertain whether a higher degree or lesser degree of document security is required to ensure that information is released only when and if appropriate.

a. **Source reliability** — The reliability of the source is an index of the consistency of the information the source provides. In all cases, source identification should be available in some form. The true identity 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 how sources are to be identified. The source shall be evaluated according to the following:

   1) RELIABLE — The reliability of the source is unquestioned or has been tested in the past.

   2) USUALLY RELIABLE — The source of information can usually be relied upon. The majority of the information provided in the past has proved 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; either experience or investigation has not yet determined authenticity or trustworthiness.

   Because the value of information stored in a criminal intelligence file is directly related to the source of such

information, the following factors should be considered in determining how to identify the source:

- 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

Whether or not confidential source identification is warranted, reports should reflect the name of the submitting agency and the reporting individual. In those cases where identifying the source by name is not practical for security reasons, a code number may be used. A confidential listing of coded sources of information can then be retained by the commanding officer of the Criminal Intelligence Section. In addition to identifying the source, it is appropriate 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.)

b. **Content validity** — The validity of the information is an index of the accuracy or truthfulness of the information. The validity of the information shall be assessed as follows:

1) CONFIRMED — The information has been corroborated by an investigator or another reliable independent 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.

The currency or timeliness of the information will always be part of this process. Confirmed information from a reliable source that is out of date may not merit addition to an intelligence system. Given the five-year purge standard (see 28 CFR § 23.20(h)), information relating to time periods of greater than five years ago should be connected to current activity before it is added to a file.

6. **Re-evaluation** — After the reliability of the source and the validity of the content have initially been determined, it is useful to re-evaluate. This process will re-evaluate and cull the information that has no potential to become intelligence matter from the rest of the information. One useful approach in this process is to have a reviewer or second analyst examine the material. Obviously, if a file is already established and the information to be added is otherwise appropriate, this step might be minimized or eliminated.

   The process will be unique to each "batch" of information. One example would be where there is doubtful information from an unreliable source, it should be disregarded and destroyed. A contrast would be confirmed information from a reliable source that, obviously, should be put into the system if it meets the criteria for entry.

   The process will be dynamic. If, as an example, confirmed information is provided by another source previously viewed as unknown and further assessment demonstrates the source obtained the information independent of any other known source, the information should probably be entered and the status of the source should be re-evaluated.

7. **Criteria application** — Information that survives re-evaluation must then be assessed to determine whether it supports a "reasonable suspicion" of the existence of a "criminal predicate." This means a determination that the information pertains to:

   a. **Individuals who**

      1) are reasonably suspected of being involved in the actual or attempted planning, organizing, financing or commission of criminal acts; or

      2) are reasonably suspected of being involved in criminal activities with known or suspected crime figures.

   b. **Organizations, businesses and groups that**

      1) are reasonably suspected of being involved in the actual or attempted planning, organizing, financing or commission of criminal acts; or

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

Information that satisfies any of these criteria should become part of the intelligence system either as a separate file or as part of an existing file.

8. **Information requiring further development**

Application of the criteria set forth above to information vetted by the re-evaluation will result in some information that may (1) have either both content validity and source reliability but which needs more development to satisfy the entry criteria; or (2) have either content validity or source reliability only; or (3) be unknown as to content and source but of sufficient potential importance to be developed if possible.

Information that does not initially meet the criteria for entry–but may be developed–should be given "temporary" status. It is recommended that retention of "temporary" information not exceed one year unless a well-documented compelling reason exists to extend this time period. An example of a compelling reason would be if several pieces of information indicate a crime has been committed by a single suspect exhibiting a unique modus operandi but more than a year is needed to identify that suspect (for example, a Unabomber-type situation).[16]

a. An individual, organization, business or group may be given "temporary" status in the following cases:

1) **Subject or entity is unidentifiable** — The subject or 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 or entity which has either:

A) **Possible criminal associations** — Individual, organization, business, or group not currently reported to be criminally active but associates with a known criminal who is reasonably suspected of being involved in illegal activities.

16. This "compelling reason" approach will typically have application in the terrorism – either domestic or international – arena. "Compelling reason" cases should be thoroughly documented as to why the information deserves retention. The category should be used sparingly, if at all. The retention of files containing "temporary" information should be approved by the agency head and the legal advisor.

B) **History of criminal conduct** — Individual, organization, business, or group not currently reported to be criminally active but has a history of criminal conduct; and the circumstances currently being reported (i.e., new position or ownership of a business) indicate they may have, again, become criminally active.

3) **Reliability and/or 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.

b. While it is appropriate to maintain temporary information in the intelligence unit because of its sensitivity, it should not be made part of the intelligence system until it satisfies the entry criteria. It should be separately maintained. Further, it is important to emphasize the need to actively "work" the temporary file(s) in an effort to determine whether it should be added to the intelligence system or be destroyed. Failure to actively "work" the files while retaining the information will suggest that the intelligence system is merely collecting information without regard to the criminal predicate requirement.

9. **Final review** — Information to be stored in the criminal intelligence file should undergo a thorough final evaluation by a designated quality control reviewer for compliance with established file input guidelines prior to being filed. The name of the person responsible for this final review and entry decision should appear in the file along with a statement of his or her basis for the decision and identification of the definable criminal conduct involved.

VI. File Content

A. **Information input** — Only information meeting an agency's criteria for file input should be stored in the criminal intelligence file. Examples of excluded material are information on an individual or group merely on the basis of race, ethnic background, religious affiliation, political affiliation, or sexual preference that does not relate directly to criminal conduct. Also excluded are associations

with individuals, businesses, or groups that are not of a criminal nature.

B. **California statutes regarding intelligence files** — California has no statutes that govern what may be contained in an intelligence file. Absent a court order, which directs what may be maintained, the 28 CFR 23 criteria should be applied. An intelligence file will often include open-source material and public record material as well as non-public information, such as investigative reports and intelligence analyses.

1. Some agencies believe that separating the files into public and non-public segments will prevent the release of intelligence information in the event a subpoena is issued. This belief is unfounded. All information requested in the subpoena may be subject to disclosure. However, intelligence information is subject to a claim of official information privilege pursuant to Article 9 of the California Evidence Code (commencing with Section 1040). A court, acting *in camera*, will review the information submitted and determine what is to be released.

2. Likewise, if the request for access to an intelligence file is in the form of a Public Records Act request (see Government Code section 6250, et seq.), the entire file will be subjected to *in camera* judicial review to determine whether and to what extent the disclosure is required.

3. The best policy is to maintain all of the information that pertains to a given subject in one file regardless whether it is open-source or public record information. Indeed, in some cases, the open-source or public information may become non-disclosable because the connection to the file subject would reveal information; this will, of course, be determined by the *in camera* review.

C. **Criminal offender record information** — At this point, it is necessary to comment about criminal offender record information ("CORI") data. (See Penal Code section 11705; Title 28, Code of Federal Regulations, Part 20.) An agency's CORI file system "should not" be incorporated into its intelligence file system. The CORI system is subject to different rules (see California Code of Regulations, Title 11, Section 703) and should be a separate file system maintained at a separate location from the intelligence file system. However, it is appropriate to place a copy of an individual's criminal history in an intelligence file. If a copy of a subject's criminal history is placed in the file, it should be checked against

the CORI file before dissemination to be certain it reflects the most recent CORI data; or, in the alternative, it should not be included in the dissemination.

D. **General rules regarding file contents** — 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 mandates the internal approval that must be completed prior to release of the information to persons outside the particular agency disseminating the information.

1. However, the classification of information, by itself, is not a defense against a subpoena duces tecum, other court processes, or a Public Records Act request. Proper classification of the information in the file will assist a court reviewing a disclosure issue in understanding how the information in the file interrelates and what impact it may have on the privacy concerns of the subjects identified in the file.

2. 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 or dissemination criteria assigned to particular documents. Documents within the intelligence files should be reviewed on an ongoing basis to ascertain whether a higher degree or lesser degree of document security is required and to ensure that information is released only when – and if – appropriate.

E. **Sensitivity** — The sensitivity of the information shall be classified according to the following standards:

1. SENSITIVE — Information, including, but not limited to, active police investigations, informant identification information, corruption, and those reports which require strict dissemination and release criteria.

2. RESTRICTED — Information obtained through intelligence channels that is not classified as sensitive and is for law enforcement use only. Restricted information may include previously classified sensitive information for which the need for a high level of security no longer exists.

3. UNCLASSIFIED — Information that is public in nature. This includes the following: (a) information to which, in its original form, the general public has or had direct access (i.e., birth and death certificates); (b) news media information, such as

newspaper, magazine, periodical clippings, and/or videotapes, dealing with specified criminal events; and (c) other open-source material (i.e., internet information).

VII. Analysis

The various steps discussed in Part V, *supra*, are, of course, the process of analyzing the data. These steps determine whether, when viewed in totality, there is reasonable suspicion that the data supports the belief the individual or organization is involved in the commission – or support of – definable criminal activity.

VIII. Information Dissemination

Agencies must adopt formalized procedures for access to and dissemination of intelligence information. These procedures should apply to requests from the agency's personnel as well as to requests from other agencies. These procedures will protect the individual's right to privacy and maintain the confidentiality of the sources and the file. Most important, strict adherence to these procedures will ensure the agency's reputation for proper handling of intelligence in the law enforcement, judicial, and non-law enforcement communities.

A. **Information dissemination policies** — The following policies should be adopted to govern the access to and dissemination of intelligence information:

1. Criminal intelligence officers shall disseminate criminal intelligence information only where there is a need to know and a right to know the information in the performance of a law enforcement activity.

    a. Except as noted in subsection A.1.b., below, officers shall disseminate criminal intelligence information only to law enforcement authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination that are consistent with these principles.

    b. Subsection A.1., above, shall not limit the dissemination of an assessment of criminal intelligence information to a government official or to any other individual, when necessary to avoid imminent danger to life or property.

2. Criminal intelligence information may only be shared with other law enforcement agencies with the approval of the commanding

officer of the Criminal Intelligence Section, or pursuant to a written policy of the Criminal Intelligence Section. The release of this information shall be based on a need to know and right to know basis. The facts establishing the requestor's need to know and right to know shall be documented in the criminal intelligence file. The agency and/or officer requesting the information, the officer approving the sharing, the law enforcement purpose for the request, the date of the request, and the date of the provision of information shall all be noted in the file. The agency and/or officer requesting the information shall agree in writing to be bound by these Standards and Procedures relating to the storage, retrieval and dissemination of the information provided.

a. In maintaining criminal intelligence information, a local law enforcement agency that adopts these Standards and Procedures shall ensure that administrative, technical, and physical safeguards (including audit trails) are adopted to ensure against unauthorized access and against intentional or unintentional damage. A record indicating who has been given information, the reason for the release of the information, and the date of each dissemination outside the Criminal Intelligence Section shall be kept. Information shall be labeled to indicate levels of sensitivity, levels of confidence, and the identity of the requesting agencies and control officials. The officer releasing information shall document in the criminal intelligence file the existence of an inquirer's need to know and right to know the information being requested, either through inquiry or by delegation of this responsibility to a properly trained participating agency, which information release is subject to routine inspection and audit procedures established by the local law enforcement agency that adopts these Standards and Procedures.

b. Criminal intelligence information shall only be shared with other members within the law enforcement agency on a need to know basis. The officer requesting the information and the justification for the request shall be noted in the file.

3. Criminal Intelligence Section personnel will not release any original intelligence documents. Whenever information from a criminal intelligence file is disclosed, in any form, either orally, in writing, or through inspection of files, the Criminal

Intelligence Section must comply with the requirements set forth above in Section A.2.

4. **Need to know** — This standard is established when the requested information is pertinent and necessary to the requesting agency in initiating, furthering, or completing the performance of a law enforcement activity.

5. **Right to know** — This standard is established when the requester is acting in an official capacity and has statutory authority to obtain the information being sought.

6. The Criminal Intelligence Section's intelligence information will be released according to the following classification and release authority levels:

   a. SENSITIVE — Information in this class may only be released with permission of the commanding officer of the Criminal Intelligence Section to law enforcement agencies that have a demonstrated right to know and need to know.

   b. RESTRICTED — Restricted information may be released by Criminal Intelligence Section personnel to law enforcement agencies that have a demonstrated right to know and need to know.

   c. UNCLASSIFIED — Any Criminal Intelligence Section personnel may release this information to any other officer within the local law enforcement agency, or any other law enforcement agency. The Chief of Police or Sheriff is the official record custodian and the Chief of Police or Sheriff must approve the release of information to the public or to the media.

B. **File integrity issues** — The integrity of the criminal intelligence file can be maintained only by strict adherence to proper access/dissemination guidelines, such as those set forth above. To eliminate unauthorized use and abuses of the system, an agency must utilize an access/dissemination form that is maintained with each stored document. This control form records the date of the request, the name of the requester and his or her right to know, the specific 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 may also be designed to record other items useful in the management of its operations–as well as providing an audit trial.

1. As cooperative efforts among agencies expand through the use of internet-based sharing systems, an added layer of access and dissemination control comes into play. The following categories or similar categories should be created:

   a. **Free access** — Other parties may enter information to existing files without authorization. The audit requirements must be maintained. Other parties may not remove or alter existing information.

   b. **Read-only access** — Other parties may see all or part of the existing information but may not enter information. Audit requirements apply.

   c. **"Pointer" access** — Other parties may enter identifiers. If the result is a match to information in the file, they do not see the information, but instead are "pointed" to a contact. Audit requirements apply.

   In both a traditional and internet-based system, the so-called "third-party rule" applies. The essence of this rule is that information developed by a source agency will not be released by a recipient agency to a third-party agency until the source agency is notified and agrees to the release. Clearly, this process is automatic in the internet-based system context because the "architecture" of such systems can build in appropriate levels of the third-party rule.

IX. Maintenance of the File

A. **Introduction** — While it is fundamentally important that intelligence files be used, it is equally important that access to these files be strictly controlled. The criminal intelligence file should be located in a secured area, with file access restricted to authorized law enforcement personnel. In connection with the term "authorized personnel," it is important to apply the "need to know/right to know" test. In other words, a person who is a sworn peace officer employed by an agency "does not" automatically have the "need to know," which would provide access to an intelligence file. Agency guidelines must require that access is case by case, rather than open on the basis of status only.

1. 28 CFR § 23.20(g) addresses the importance of file security as follows:

   "A project maintaining criminal intelligence information shall ensure that administrative, technical, and physical

safeguards (including audit trails) are adopted to insure against unauthorized access and against intentional or unintentional damage. A record indicating who has been given information, the reason for release of the information, and the date of each dissemination outside the project shall be kept. Information shall be labeled to indicate levels of sensitivity, levels of confidence, and the identity of submitting agencies and control officials. Each project must establish written definitions for the need to know and right to know standards for dissemination to other agencies as provided in paragraph (e) of this section. The project is responsible for establishing the existence of an inquirer's need to know and right to know the information being requested either through inquiry or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project. Each intelligence project shall assure that the following security requirements are implemented:

"(1) Where appropriate, projects must adopt effective and technologically advanced computer software and hardware designs to prevent unauthorized access to the information contained in the system;

"(2) The project must restrict access to its facilities, operating environment and documentation to organizations and personnel authorized by the project;

"(3) The project must store information in the system in a manner such that it cannot be modified, destroyed, accessed, or purged without authorization;

"(4) The project must institute procedures to protect criminal intelligence information from unauthorized access, theft, sabotage, fire, flood, or other natural or man-made disaster;

"(5) The project must promulgate rules and regulations based on good cause for implementing its authority to screen, reject for employment, transfer, or remove personnel authorized to have direct access to the system; and

"(6) A project may authorize and utilize remote (off-premises) system data bases to the extent that they comply with these security requirements."

B. **File security policies**

1. Criminal intelligence files will be physically secured in locked cabinets or in electronic files that are equipped with security

protection measures. Those files and databases will be secured during off-hours and when the office is vacant.

2. Key access to the Criminal Intelligence Section will only be granted to assigned section personnel.

3. Locks, combinations and system passwords will be changed upon the transfer of any member.

4. Criminal Intelligence Section personnel will adopt a "clean desk" policy to include the removal of sensitive documents from view when not in use. The orientation of computer monitors will be such as to preclude casual observation by visitors and there will be control of sensitive conversations.

X. Review and Purge Procedures

A. **Introduction** — Information stored in the criminal intelligence file must be reviewed to determine whether it is current, accurate, relevant and complete (i.e., contains all source materials or copies of such materials) and whether it continues to meet the needs and objectives of the responsible agency. Under 28 CFR 23, an intelligence file must be purged at the end of a five-year period unless it had information added that verifies the continued validity of the criminal predicate (or additional criminal predicates) that initially justified the creation of the file. Also, if before the five-year period expires the agency maintaining the file learns that any information upon which it relied for creating the file is no longer valid or was not initially valid, that information must be purged and the file's validity without consideration of that information must be evaluated.

B. **Review and purge policies**

1. Reviewing and purging of all information that is contained in the Criminal Intelligence Section's criminal intelligence files and kept pursuant to these Standards and Procedures will be done on an ongoing basis, but, at a minimum, will be accomplished annually. The dates when reviews occurred shall be noted in the criminal intelligence file. The maximum retention period is five (5) years, and a criminal intelligence file must be purged after five years unless the information in that criminal intelligence file has been updated consistent with these Standards and Procedures. The Criminal Intelligence Section may update the criminal intelligence file and extend the retention period at any

time, based on reasonable suspicion of new criminal activity documented in the criminal intelligence file.

2. The decision to purge information should be guided by the following considerations:

   a. Whether or not the information in the criminal intelligence file continues to comply with the reasonable suspicion standard as defined above in Section III. Also, if the Criminal Intelligence Section learns, prior to the five-year period for purging, that any information that it relied upon for creating a criminal intelligence file is no longer valid or was initially invalid, that information must be purged and the criminal intelligence file's validity without consideration of that information must be evaluated.

   b. Defined retention periods for criminal intelligence files.

   c. Specific credible threats to government officials and/or law enforcement officers.

3. Any information that is found to be collected or retained in violation of this subsection, or is found to be inaccurate, misleading, or obsolete, shall be purged. ***Purged means destroyed***, and not simply put into another file system. Any recipient agencies shall be advised of such changes and that the subject information has been purged.

C. **Practical considerations**

In implementing the review and purge policies set forth above, some consideration should be given to the following:

1. <u>Utility of the information</u>

   Who uses the information?

   How often is the information used?

   For what purpose is the information being used?

2. <u>Timeliness and appropriateness</u>

   Is an investigation still ongoing?

   Is the information outdated?

   Is the information still relevant to the needs and objectives of the responsible agency?

Is the information still relevant to the purpose for which it was collected and stored?

3. Accuracy and completeness

   Is the information still valid?

   Is the information still adequate for identification purposes?

   Has the continued validity of the data been determined through investigation or analysis?

D. **Other considerations regarding records purging**

1. It is the responsibility of each state and local agency to ensure that their obsolete records are destroyed in accordance with applicable laws, rules, and state or local policy.

   a. Sections 4840.4 and 4841.3 of the State Administrative Manual define "confidential information" as "Information maintained by state agencies that is exempt from disclosure under the provisions of the California Public Records Act (Government Code Sections 6250-6265) or other applicable state or federal laws."

   b. Section 4841.3 of the State Administrative Manual defines "sensitive information" as "information maintained by state agencies that requires special precautions to protect from unauthorized use, access, disclosure, modification, loss, or deletion. Sensitive information may be either public or confidential. It is information that requires a higher than normal assurance of accuracy and completeness. Thus the key factor for sensitive information is that of integrity. Typically, sensitive information includes records of agency financial transactions and regulatory actions."

2. In no situation should the names or any other identifying information regarding those whose files have been purged continue to exist. **Destroy means destroy**. If the names or identifications are not destroyed, then the fact that the person was reasonably suspected continues to exist and no meaningful purge has occurred. Purges must be structured so that they are system wide.

3. In rare instances, state statute (see, e.g., Government Code sections 26202 [re county boards of supervisors] and 34090 [re city councils])[17] or local ordinance or code will preclude

17. See Appendix B. In general, these statutes provide that records less than two years old should not be destroyed without the approval of the governing body.

timely destruction (i.e., purge) of documents. In such cases, the documents should be removed from the intelligence files at the time dictated by the purge requirements, sealed, signed, dated, and stored in a non-accessible location until such time as the particular legal provision allows destruction.

XI. Closing Comments

The intelligence function is a necessary "privilege" that law enforcement enjoys in ensuring public safety and enforcing the criminal laws. Because it is a privilege, it must be carried out carefully. Inattention to the rules governing the function will have disastrous consequences for an agency and will reduce its ability to discharge its responsibility in an optimal manner. Strict adherence to these Standards and Procedures is the only way to manage an intelligence function.

Section Two

Criminal Intelligence Operational Activities

I. Authorized Intelligence Operational Activities

A. **Graduated Levels**: The Criminal Intelligence Section follows a graduated level of investigative activity in order to provide the necessary flexibility to act well in advance of the commission of a planned criminal act. The three levels of investigative activity are: (1) Initial Lead Investigations, (2) Preliminary Investigations, and (3) Open Investigations. Whether it is appropriate to open an investigation immediately, or instead first engage in a limited follow up of lead information, depends on the circumstances presented. If the available information shows at the outset that the threshold standard for a Preliminary or Open Investigation is satisfied, then approval to conduct the appropriate investigation activity may be requested immediately, without progressing through the more limited investigative stage. However, if the reasonable suspicion standard has not been met, only an Initial Lead Investigation may go forward.

1. Initial Lead Investigations: The lowest level of investigative activity is the prompt and limited follow up of initial leads, many of which are initiated by the public. Follow up on leads should be undertaken whenever information is received of a suspicious nature that some follow up as to the possibility of criminal activity is warranted. This limited activity should be conducted with an emphasis toward promptly determining whether further investigation, either a Preliminary Investigation or an Open Investigation, should be conducted. Many initial investigative leads from the public and other sources are expected to be somewhat vague and may not meet the reasonable suspicion standard for a Preliminary or Open Investigation. However, public safety demands a limited but prompt follow up investigation. The authority to conduct inquiries short of a Preliminary or Open Investigation allows the Criminal Intelligence Section to respond in a measured way to ambiguous or incomplete information. An Initial Lead Investigation may commence upon approval by the Criminal Intelligence Section's commanding officer.

   a. *PERMITTED INVESTIGATIVE TECHNIQUES*: The following investigative techniques are authorized for Initial Lead Investigations: (1) examination of records available to the public (open source); (2) examination of local law enforcement agency records; (3) examination of available federal, state, local government records, etc.; (4) interview of

the person reporting; (5) interview of the potential subject; (6) Interview of the witness; and (7) monitoring.

b. *TIME FOR COMPLETION*: Initial Lead Investigations shall be completed within one hundred twenty (120) days from the date of receipt of the specific lead.

2. Preliminary Investigations: The next level of investigative activity, a Preliminary Investigation, should be undertaken when there is information or an allegation which indicates the possibility of criminal activity. Preliminary Investigations are based on reasonable suspicion only and are for the purpose of determining whether or not the information or allegation can be developed to the point of reliability. A Preliminary Investigation may be initiated when the local law enforcement agency that adopts these Standards and Procedures possesses a reasonable suspicion that the individual and/or organization is involved in a definable criminal activity or enterprise. A Preliminary Investigation may commence upon approval by the Criminal Intelligence Section's commanding officer.

   a. *PERMITTED INVESTIGATIVE TECHNIQUES*: A Preliminary Investigation shall not involve the use of electronic surveillance that requires a court order. All other lawful investigative methods are authorized.

   b. *TIME FOR COMPLETION*: Preliminary Investigations shall be completed within two hundred forty (240) days.

3. Open Investigations: The commencement of each Open Investigation shall be approved by the Criminal Intelligence Section's commanding officer. An Open Investigation may be initiated when the local law enforcement agency that adopts these Standards and Procedures possesses a reasonable suspicion, based upon reliable information, that the individual and/or organization is involved in a definable criminal activity or enterprise. All lawful investigative techniques may be used in an Open Investigation.

B. **Limits on Investigations of Political Demonstrations**: The Criminal Intelligence Section shall not conduct any investigation of a planned political demonstration, march, rally or other similar public event, including an act of non-violent civil disobedience, unless the local law enforcement agency possesses a reasonable suspicion that an individual and/or organization at such a planned event will be involved in a definable criminal activity or enterprise. Any Criminal Intelligence Section investigation of a planned political

demonstration, march, rally or other similar public event, including an act of non-violent civil disobedience, must be approved of, in writing, by the Criminal Intelligence Section's commanding officer prior to the event.

1. Exceptions: The limitation set forth above in Section B does not apply in the following circumstances:

   a. Any approved Criminal Intelligence Section investigation of a targeted individual and/or organization that has an undercover officer assigned to the investigation in compliance with Section XII.

   b. Routine assignments to provide traffic control, crowd management or other traditional safety measures at a planned political demonstration, march, rally or other similar public event, including an act of non-violent civil disobedience.

2. Videotaping at Political Demonstrations: Routine assignments may videotape or photograph a planned political demonstration, march, rally or other similar public event, including an act of non-violent civil disobedience, for either crowd control training or for an evidentiary purpose discussed below in Section B.2.a. However, the Criminal Intelligence Section may only videotape or photograph a planned political demonstration, march, rally or other similar public event, including an act of non-violent civil disobedience, under the following circumstances:

   a. The videotape or photograph is taken to obtain evidence that is reasonably likely to be used in administrative, civil, or criminal proceedings or investigations; and,

   b. The videotape is taken at an event that has been authorized by the Criminal Intelligence Section's commanding officer pursuant to Section B above or by the Chief of Police or Sheriff in Section XII.

II. Use of Undercover Criminal Intelligence Officers

A. **Standard for Using Undercover Officers in Criminal Intelligence Preliminary or Open Investigations**:

1. Reasonable Suspicion Standard: The Chief of Police or Sheriff may approve the use of an undercover officer in a Criminal Intelligence Section Preliminary or Open Investigation regarding a targeted individual and/or organization when the

local law enforcement agency that adopts these Standards and Procedures possesses a reasonable suspicion that the individual and/or organization is involved in a definable criminal activity or enterprise. In making this determination, participation in political protest, non-violent civil disobedience, or public expression through demonstrations do not, by themselves, constitute sufficient information to justify assigning an undercover officer to a Criminal Intelligence Section Preliminary or Open Investigation.

2. Standard for Infiltrating a Non-target Group: As part of a Criminal Intelligence Section Preliminary or Open Investigation regarding a target group or individual that meets the reasonable suspicion standard set forth above in Section A.1, there may be circumstances when the local law enforcement agency that adopts these Standards and Procedures possesses a legitimate law enforcement need to use an undercover officer to infiltrate a non-target organization that is not suspected of any criminal activity. As part of an approved Criminal Intelligence Section Preliminary or Open Investigation, the Chief of Police or Sheriff may approve the infiltration of a non-target group with an undercover officer when there is a reasonable basis for believing that the presence of an undercover officer in the non-target organization will enable the undercover officer to infiltrate the target organization as evidenced by the following factors:

   a. Members of the target organization are also members of the non-target organization;

   b. The target organization recruits members from the active members of the non-target organization;

   c. Membership in the non-target organization is a condition of membership in the target organization; or,

   d. There is a substantial link between the non-target organization and target organization, equal to those described above, which otherwise justifies the undercover officer's infiltration of the non-target organization; provided, however, that this substantial link shall not be based solely on the evidence that: (1) the non-target organization espouses or holds the same political, social or economic positions as the target organization (e.g. a non-violent organization which opposes nuclear power plants shall not be infiltrated in order to infiltrate a target organization which opposes nuclear plants by violent means unless there are

other factors present); or (2) the non-target organization shares the same racial, religious or other status or concerns with the target organization.

B. **Requesting and Authorizing an Undercover Officer for a Criminal Intelligence Section Preliminary or Open Investigation**:

1. Requesting an Undercover Officer: The Criminal Intelligence Section's commanding officer must request approval from the Chief of Police or Sheriff prior to using an undercover officer in a Criminal Intelligence Section Preliminary or Open Investigation. The commander's request to the Chief of Police or Sheriff shall be in writing, and shall include the following:

   a. All information relevant to establishing the existence of the reasonable suspicion standard identified above in Section A.1;

   b. If the request seeks approval for the undercover officer to infiltrate a non-target group, then all information relevant to establishing the need for such an infiltration pursuant to the standard identified above in Section A.2.a-d;

   c. The requested duration of the assignment, not to exceed one year.

2. Chief of Police or Sheriff's Response to the Request for Using an Undercover Officer: The Chief of Police or Sheriff shall respond in writing to all requests by the Criminal Intelligence Section's commanding officer seeking approval for the use of an undercover officer in a Criminal Intelligence Section Preliminary or Open Investigation. If the Chief of Police or Sheriff approves the request, the written approval must include the following:

   a. Specifying the individual or organization that is the target of the undercover officer's investigation;

   b. Setting forth limitations, if any, on the activities which can be engaged in by the undercover officer with regard to the target individual or organization;

   c. Imposing a time limit on the undercover officer's assignment, which, however, cannot exceed a period of one year with quarterly review by the Chief of Police or Sheriff; and,

   d. If the Chief of Police or Sheriff also approves an infiltration of a non-target organization, then the written approval shall include the following additional terms:

1) Specifying the non-target organization that may be infiltrated;

2) Specifying the reasonable basis for believing that the presence of the undercover officer in the non-target organization will enable the undercover officer to infiltrate the target organization as evidenced by the factors set forth above in Section A.2.a-d;

3) Setting forth limitations, if any, on the activities which can be engaged in by the undercover officer with regard to the non-target organization; and,

4) Imposing a time limit on the undercover officer's infiltration of the non-target organization, which cannot exceed a period of one year with quarterly review by the Chief of Police or Sheriff.

3. Exceptions: In an emergency involving a life threatening situation, where the Chief of Police or Sheriff is unavailable, use of an undercover officer in a Criminal Intelligence Section Preliminary or Open Investigation may be commenced with the approval of the Criminal Intelligence Section's commanding officer. In such cases, notification to the Chief of Police or Sheriff shall be made as soon as possible and written approval from the Chief of Police or Sheriff shall be secured within 72 hours.

C. **Incidental Contact Groups and Incidental Contact Activities**: During the course of an approved undercover officer assignment to a Preliminary or Open Investigation, an undercover criminal intelligence officer may be required, for purposes of maintaining his or her cover, to attend the meetings, functions, demonstrations or other activities (whether public or private) of another group or organization other than the target or non-target organization. Such a group or organization shall be known as an incidental contact group. The undercover criminal intelligence officer may also be required, for purposes of maintaining his or her cover, to attend events with members of the target or non-target group, such as religious events, public demonstrations, political events, public forums, or academic institution activities. Such events shall be known as incidental contact activities. An undercover criminal intelligence officer may attend and/or participate in events involving incidental contact groups or incidental contact activities under the following circumstances:

1. Maintaining Cover: The criminal intelligence officer's purpose for attending and/or participating in an incidental contact activity or incidental contact group event is to maintain his or her cover during the assignment regarding the Preliminary or Open Investigation involving a target or non-target group.

2. Reporting to Commander: Once an undercover officer is present on two occasions at an incidental contact group's event, or on two occasions at an incidental contact activity, the undercover officer shall report his actions to the Criminal Intelligence Section's commanding officer. The undercover officer shall not attend any more of the incidental contact group's events, or the incidental contact activities, without the approval of the Criminal Intelligence Section's commanding officer. This approval shall only be given if the Criminal Intelligence Section's commanding officer determines that further contact by the undercover criminal intelligence officer with the incidental contact group or activity is necessary to maintain the undercover officer's cover pursuant to section C.1 above.

3. Follows additional limitations: The criminal intelligence officer follows the additional limitations set forth in Section XIII.

D. **Chief of Police or Sheriff's Periodic Review of Active Undercover Assignments**:

1. Scope and frequency of Chief of Police or Sheriff's periodic review: The Chief of Police or Sheriff shall conduct quarterly reviews of all active criminal intelligence Preliminary or Open Investigations using an undercover officer to ensure continued compliance with the standards set forth above in Section A. Such compliance shall be assessed, at the time of review, based on (i) all information considered at the time of initial authorization, (ii) all information considered in previous reviews and re-authorizations, (iii) all information produced by the undercover operations, and (iv) information on all activities of the undercover officer during the intervening period, including all organizations and individuals with whom the officer has had contact. The results of these quarterly reviews shall be documented in a memo.

2. Termination of undercover officer's assignment: If the Chief of Police or Sheriff determines, based on his or her review, that an undercover officer's active criminal intelligence assignment to a Preliminary or Open Investigation no longer complies with the standards set out above in Section A, then the Chief of Police

or Sheriff shall order termination of the assignment. Any such termination shall be documented in a memo. The memo may specify the limited period of time that the undercover officer has to cease his or her undercover assignment.

E. **Re-authorization of Undercover Officer's Use in a Criminal Intelligence Section Preliminary or Open Investigation**: The Chief of Police or Sheriff may re-authorize an undercover officer's use in a Criminal Intelligence Section Preliminary or Open Investigation if the Chief of Police or Sheriff, considering all available information, concludes that the standards set forth above in Section A are still present. Any re-authorization shall comply with the form and content requirements set forth above in Section B. Additionally, if the re-authorization includes infiltration of a non-target organization, the written re-authorization shall include an explanation as to why the target organization has not been infiltrated, what steps have been taken to accomplish such infiltration, and specific information supporting a continued justification for the non-target organization's infiltration based on the standards set forth above in Section A.2.a-d. The Chief of Police or Sheriff's decision to re-authorize such an assignment shall be documented in a memo.

F. **Document Retention for Audits**: All documents prepared by local law enforcement agency staff pursuant to Section XII shall be retained by the Chief of Police or Sheriff in a file separate from any criminal intelligence files, and they shall be maintained for review during annual audits.

III. Additional Limitations on Undercover Criminal Intelligence Officers

A. **Reasonable suspicion requirement** — No criminal intelligence files shall be gathered through an undercover assignment concerning persons or organizations as to which there is no reasonable suspicion that they or the organization is involved in any definable criminal activity or enterprise.

B. **Public forums** — Undercover officers used in criminal intelligence assignments shall observe the following guidelines when present at any religious events, public demonstrations, political events, public forums, or academic institutions:

1. Undercover officers shall not assume leadership roles, advocate any course of conduct, or initiate civil disobedience;

2. Undercover officers shall not engage in any acts of harassment, intimidation, or disruption of any events, meetings, rallies, forums, classes, or similar events he or she attends as part of the undercover role;

3. Undercover officers shall not intentionally attend meetings involving any individual or organization and a person that individual or organization is consulting in a manner which gives rise to a statutory privilege pursuant to Evidence Code Sections 954, 980, 994, 1012, or 1033;

4. Undercover officers shall report the fact of their attendance at any of the locations or under any of the circumstances set forth above Section B. With the exception of privileged situations as to which there is no waiver of privilege, the undercover officer shall record and report only those aspects of the event relevant to the undercover investigation or necessary to correctly understand the context of relevant events; and as to privileged situations where there was no waiver, the undercover officer shall prepare no reports regarding that meeting.

IV. Standards and Responsibilities of Commanders of Criminal Intelligence Sections

A. **Training of undercover officers**: The Criminal Intelligence Section's commanding officer shall ensure each undercover officer assigned to this unit is familiar with these Standards and Procedures and is trained regarding acceptable standards of conduct.

B. **Maintaining criminal intelligence files**: The Criminal Intelligence Section's commanding officer, or his or her designee, shall be responsible for maintaining all criminal intelligence files and temporary files within the section. The commanding officer shall also be responsible for the policies regarding dissemination of the information in those files. To accomplish these responsibilities, the commanding officer shall establish written policies and procedures which shall be approved by the Chief of Police or Sheriff. These policies and procedures shall comply with 28 CFR § 23.20(f), (g), (h), (l), (m) and (n).

C. **Annual criminal intelligence file and assignment review**: Independent of the annual audit described in Section XV of these Standards and Procedures, the Criminal Intelligence Section's commanding officer shall annually review all of the section's criminal intelligence files. The Criminal Intelligence Section's commanding officer shall also annually review all of the section's ongoing

assignments where undercover criminal intelligence officers have been deployed. The commanding officer shall certify in writing to the Chief of Police or Sheriff that the criminal intelligence files and ongoing assignments deploying an undercover criminal intelligence officer are in compliance with the Standards and Procedures, or will take all those steps necessary to bring those files and assignments into compliance.

D. **Document retention for audits**: The commanding officer's written certification described above in Section C shall be retained for review during annual audits.

V. Auditing and Oversight

A. **Annual audit**: At least annually, the Chief of Police or Sheriff shall appoint two department Captains (hereinafter the "audit committee") to audit the operations of the Criminal Intelligence Section for compliance with these Standards and Procedures. The audit committee may enlist the assistance of at least one department administrative support staff member who shall be subject to a background examination and possess the requisite auditing and management expertise to ensure compliance with these Standards and Procedures.

B. **Scope of annual audit**: The annual audit shall consist of, but not be limited to, the following:

1. A review of all Criminal Intelligence Section regulations, rules and policies;
2. A review of all Criminal Intelligence Section Initial Lead Investigations, Preliminary Investigations, Open Investigations, and investigations in connection with demonstrations;
3. A review of all criminal intelligence and temporary files;
4. A review of all documents prepared pursuant to Section XII of these Standards and Procedures;
5. A review of the commanding officer's annual written certification conducted pursuant to Section VII of these Standards and Procedures;
6. Oral interviews with Criminal Intelligence personnel. These oral interviews may cover all aspects of compliance with these Standards and Procedures, as well as the following specific topics:

a. Discuss an officer's undercover criminal intelligence assignments during the past year, and discuss whether these assignments resulted in obtaining any useful criminal intelligence information.

b. Discuss with the commanding officer the results of his or her annual criminal intelligence file and assignment review prepared pursuant to Section XIV of these Standards and Procedures;

C. **Surprise inspections**: The audit committee or their designated administrative auditor(s) may at any time conduct surprise audits or inspections as deemed appropriate to monitor compliance with these Standards and Procedures.

D. **Written audit report**: Based upon the audit, the administrative auditor(s) under the supervision of the audit committee, shall prepare a confidential written audit report for the local law enforcement agency's Chief of Police or Sheriff. This report shall set forth the nature of the audit and the audit committee's findings regarding the Criminal Intelligence Section's compliance with these Standards and Procedures.

E. **Public report**: From the above confidential report, the Chief of Police or Sheriff may prepare a public report of the audit on the preceding year's activities of the Criminal Intelligence Section.

VI. Closing Comments

While intelligence operational activities can certainly support law enforcement efforts to safeguard the public from terrorist, organized crime, criminal gang and other conspiratorial threats, law enforcement must nevertheless remain mindful of the public presentiment that its intelligence operational activities can be improperly employed against legitimate political, religious, cultural or social activities. These Model Standards and Procedures comprise the California Attorney General's best assessment of the relevant legal authorities and are presented to assist law enforcement executives and their intelligence operations commanders in the conduct of intelligence operational activities with a view to upholding our fundamental freedoms and rights.

Appendix A

PART 23 - CRIMINAL INTELLIGENCE SYSTEMS OPERATING POLICIES

Authority: 42 U.S.C. 3782(a); 42 U.S.C. 3789g(c).

Source: 58 FR 48452 [Sept. 16, 1993].

§ 23.1. Purpose.

The purpose of this regulation is to assure that all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, et seq., as amended (Pub. L. 90-351, as amended by Pub. L. 91-644, Pub. L. 93-83, Pub. L. 93-415, Pub. L. 94-430, Pub. L. 94-503, Pub. L. 95-115, Pub. L. 96-157, Pub. L. 98-473, Pub. L. 99-570, Pub. L. 100-690, and Pub. L. 101-647), are utilized in conformance with the privacy and constitutional rights of individuals.

§ 23.2. Background.

It is recognized that certain criminal activities including but not limited to loan sharking, drug trafficking, trafficking in stolen property, gambling, extortion, smuggling, bribery, and corruption of public officials often involve some degree of regular coordination and permanent organization involving a large number of participants over a broad geographical area. The exposure of such ongoing networks of criminal activity can be aided by the pooling of information about such activities. However, because the collection and exchange of intelligence data necessary to support control of serious criminal activity may represent potential threats to the privacy of individuals to whom such data relates, policy guidelines for Federally funded projects are required.

§ 23.3. Applicability.

(a) These policy standards are applicable to all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, et seq., as amended (Pub. L. 90-351, as amended by Pub. L. 91-644, Pub. L. 93-83, Pub. L. 93-415, Pub. L. 94-430, Pub. L. 94-503, Pub. L. 95-115, Pub. L. 96-157, Pub. L. 98-473, Pub. L. 99-570, Pub. L. 100-690, and Pub. L. 101-647).

(b) As used in these policies: (1) Criminal Intelligence System or Intelligence System means the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information; (2) Interjurisdictional Intelligence System means an intelligence system which involves two or more participating agencies representing different governmental units or jurisdictions; (3) Criminal Intelligence Information means data which has been evaluated to determine

that it: (i) Is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and (ii) meets criminal intelligence system submission criteria; (4) Participating Agency means an agency of local, county, State, Federal, or other governmental unit which exercises law enforcement or criminal investigation authority and which is authorized to submit and receive criminal intelligence information through an interjurisdictional intelligence system. A participating agency may be a member or a nonmember of an interjurisdictional intelligence system; (5) Intelligence Project or Project means the organizational unit which operates an intelligence system on behalf of and for the benefit of a single agency or the organization which operates an interjurisdictional intelligence system on behalf of a group of participating agencies; and (6) Validation of Information means the procedures governing the periodic review of criminal intelligence information to assure its continuing compliance with system submission criteria established by regulation or program policy.

§ 23.20. Operating principles.

(a) A project shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.

(b) A project shall not collect or maintain criminal intelligence information about the political, religious or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.

(c) Reasonable Suspicion or Criminal Predicate is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise. In an interjurisdictional intelligence system, the project is responsible for establishing the existence of reasonable suspicion of criminal activity either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.

(d) A project shall not include in any criminal intelligence system information which has been obtained in violation of any applicable Federal, State, or local law or ordinance. In an interjurisdictional intelligence system, the project is responsible for establishing that no information is entered in violation

of Federal, State, or local laws, either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.

(e) A project or authorized recipient shall disseminate criminal intelligence information only where there is a need to know and a right to know the information in the performance of a law enforcement activity.

(f)(1) Except as noted in paragraph (f)(2) of this section, a project shall disseminate criminal intelligence information only to law enforcement authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination which are consistent with these principles.

(2) Paragraph (f)(1) of this section shall not limit the dissemination of an assessment of criminal intelligence information to a government official or to any other individual, when necessary, to avoid imminent danger to life or property.

(g) A project maintaining criminal intelligence information shall ensure that administrative, technical, and physical safeguards (including audit trails) are adopted to insure against unauthorized access and against intentional or unintentional damage. A record indicating who has been given information, the reason for release of the information, and the date of each dissemination outside the project shall be kept. Information shall be labeled to indicate levels of sensitivity, levels of confidence, and the identity of submitting agencies and control officials. Each project must establish written definitions for the need to know and right to know standards for dissemination to other agencies as provided in paragraph (e) of this section. The project is responsible for establishing the existence of an inquirer's need to know and right to know the information being requested either through inquiry or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project. Each intelligence project shall assure that the following security requirements are implemented:

(1) Where appropriate, projects must adopt effective and technologically advanced computer software and hardware designs to prevent unauthorized access to the information contained in the system;

(2) The project must restrict access to its facilities, operating environment and documentation to organizations and personnel authorized by the project;

(3) The project must store information in the system in a manner such that it cannot be modified, destroyed, accessed, or purged without authorization;

(4) The project must institute procedures to protect criminal intelligence information from unauthorized access, theft, sabotage, fire, flood, or other natural or man-made disaster;

(5) The project must promulgate rules and regulations based on good cause for implementing its authority to screen, reject for employment, transfer, or remove personnel authorized to have direct access to the system; and

(6) A project may authorize and utilize remote (off-premises) system data bases to the extent that they comply with these security requirements.

(h) All projects shall adopt procedures to assure that all information which is retained by a project has relevancy and importance. Such procedures shall provide for the periodic review of information and the destruction of any information which is misleading, obsolete or otherwise unreliable and shall require that any recipient agencies be advised of such changes which involve errors or corrections. All information retained as a result of this review must reflect the name of the reviewer, date of review and explanation of decision to retain. Information retained in the system must be reviewed and validated for continuing compliance with system submission criteria before the expiration of its retention period, which in no event shall be longer than five (5) years.

(i) If funds awarded under the Act are used to support the operation of an intelligence system, then:

(1) No project shall make direct remote terminal access to intelligence information available to system participants, except as specifically approved by the Office of Justice Programs (OJP) based on a determination that the system has adequate policies and procedures in place to insure that it is accessible only to authorized systems users; and

(2) A project shall undertake no major modifications to system design without prior grantor agency approval.

(j) A project shall notify the grantor agency prior to initiation of formal information exchange procedures with any Federal, State, regional, or other information systems not indicated in the grant documents as initially approved at time of award.

(k) A project shall make assurances that there will be no purchase or use in the course of the project of any electronic, mechanical, or other device for surveillance purposes that is in violation of the provisions of the Electronic Communications Privacy Act of 1986, Public Law 99-508, 18 U.S.C. 2510-2520, 2701-2709 and 3121-3125, or any applicable State statute related to wiretapping and surveillance.

(l) A project shall make assurances that there will be no harassment or interference with any lawful political activities as part of the intelligence operation.

(m) A project shall adopt sanctions for unauthorized access, utilization, or disclosure of information contained in the system.

(n) A participating agency of an interjurisdictional intelligence system must maintain in its agency files information which documents each submission to the system and supports compliance with project entry criteria. Participating agency files supporting system submissions must be made available for reasonable audit and inspection by project representatives. Project representatives will conduct participating agency inspection and audit in such a manner so as to protect the confidentiality and sensitivity of participating agency intelligence records.

(o) The Attorney General or designee may waive, in whole or in part, the applicability of a particular requirement or requirements contained in this part with respect to a criminal intelligence system, or for a class of submitters or users of such system, upon a clear and convincing showing that such waiver would enhance the collection, maintenance or dissemination of information in the criminal intelligence system, while ensuring that such system would not be utilized in violation of the privacy and constitutional rights of individuals or any applicable state or federal law.

§ 23.30. Funding guidelines.

The following funding guidelines shall apply to all Crime Control Act funded discretionary assistance awards and Bureau of Justice Assistance (BJA) formula grant program subgrants, a purpose of which is to support the operation of an intelligence system. Intelligence systems shall only be funded where a grantee/subgrantee agrees to adhere to the principles set forth above and the project meets the following criteria:

(a) The proposed collection and exchange of criminal intelligence information has been coordinated with and will support ongoing or proposed investigatory or prosecutorial activities relating to specific areas of criminal activity.

(b) The areas of criminal activity for which intelligence information is to be utilized represent a significant and recognized threat to the population and:

(1) Are either undertaken for the purpose of seeking illegal power or profits or pose a threat to the life and property of citizens; and

(2) Involve a significant degree of permanent criminal organization; or

(3) Are not limited to one jurisdiction.

(c) The head of a government agency or an individual with general policy making authority who has been expressly delegated such control and supervision by the head of the agency will retain control and supervision of information collection and dissemination for the criminal intelligence system. This official shall certify in writing that he or she takes full responsibility and will be accountable for the information maintained by and disseminated from the system and that the operation of the system will be in compliance with the principles set forth in § 23.20.

(d)(1) Where the system is an interjurisdictional criminal intelligence system, the governmental agency which exercises control and supervision over the operation of the system shall require that the head of that agency or an individual with general policymaking authority who has been expressly delegated such control and supervision by the head of the agency:

(i) Assume official responsibility and accountability for actions taken in the name of the joint entity, and

(ii) Certify in writing that the official takes full responsibility and will be accountable for insuring that the information transmitted to the interjurisdictional system or to participating agencies will be in compliance with the principles set forth in § 23.20.

(2) The principles set forth in §§ 23.20 shall be made part of the by-laws or operating procedures for that system. Each participating agency, as a condition of participation, must accept in writing those principles which govern the submission, maintenance and dissemination of information included as part of the interjurisdictional system.

(e) Intelligence information will be collected, maintained and disseminated primarily for State and local law enforcement efforts, including efforts involving Federal participation.

<u>§ 23.40. Monitoring and auditing of grants for the funding of intelligence systems.</u>

(a) Awards for the funding of intelligence systems will receive specialized monitoring and audit in accordance with a plan designed to insure compliance with operating principles as set forth in §§ 23.20. The plan shall be approved prior to award of funds.

(b) All such awards shall be subject to a special condition requiring compliance with the principles set forth in §§ 23.20.

(c) An annual notice will be published by OJP which will indicate the existence and the objective of all systems for the continuing interjurisdictional exchange of criminal intelligence information which are subject to the 28 CFR part 23 Criminal Intelligence Systems Policies.

Appendix B

SELECTED GOVERNMENT CODE SECTIONS

§ 26202. Authorizing destruction of records more than two years old

The board may authorize the destruction or disposition of any record, paper, or document which is more than two years old and which was prepared or received in any manner other than pursuant to a state statute or county charter. The board may authorize the destruction or disposition of any record, paper or document which is more than two years old, which was prepared or received pursuant to state statute or county charter, and which is not expressly required by law to be filed and preserved if the board determines by four-fifths (4/5) vote that the retention of any such record, paper or document is no longer necessary or required for county purposes. Such records, papers or documents need not be photographed, reproduced or microfilmed prior to destruction and no copy thereof need be retained.

Added Stats 1947 ch 424 § 1. Amended Stats 1957 ch 1180 § 1; Stats 1963 ch 1123 § 1.

§ 34090. Authority of head of city department to destroy city records; Exceptions; Authority provided in §§ 34090.5 not limited or qualified

Unless otherwise provided by law, with the approval of the legislative body by resolution and the written consent of the city attorney the head of a city department may destroy any city record, document, instrument, book or paper, under his charge, without making a copy thereof, after the same is no longer required.

This section does not authorize the destruction of:

(a) Records affecting the title to real property or liens thereon.

(b) Court records.

(c) Records required to be kept by statute.

(d) Records less than two years old.

(e) The minutes, ordinances, or resolutions of the legislative body or of a city board or commission.

This section shall not be construed as limiting or qualifying in any manner the authority provided in Section 34090.5 for the destruction of records, documents, instruments, books and papers in accordance with the procedure therein prescribed.

Added Stats 1949 ch 79 § 1; Amended Stats 1955 ch 1198 § 2; Stats 1975 ch 356 § 1.