EMERGENCY OPERATIONS BUREAU
UNIT ORDER # 5

INTELLIGENCE GUIDELINES

APPROVED: _____

ERIC G. PARRA, CAPTAIN (DATE)

The Emergency Operations Bureau collects criminal intelligence in support of the overall mission of the department to protect the public through suppression of criminal activity. The EOB maintains its criminal intelligence information in a state of the art computerized system that contains several layers of security. Where the word "file" is utilized within these guidelines the meaning is an encrypted, password and firewall protected electronic "file".

A. Criminal Intelligence: Definition

Criminal intelligence consists of identifiable data on the activities and associations of individuals, groups, businesses and organizations either known or believed to be (reasonable suspicion) involved in criminal acts of threatening, planning, organizing or financing criminal acts.

B. Criminal Intelligence System Mission: Definition

The mission of the Criminal Intelligence System is to provide criminal intelligence support which meets the needs of the Department in carrying out its efforts to protect the public and maintain their safety through suppression of criminal activity.

C. Criminal Intelligence System File Content

Only information meeting the authorized file criteria will be stored in the Criminal Intelligence System. These materials may include documents of criminal intelligence such as informant statements, confidential field reports, special intelligence analysis and other materials not available to the public. Additionally, materials such as media reports and public documents may be commingled with criminal intelligence reports.

The Criminal Intelligence System **shall not** contain information about political, religious, or social views, associations, or activities except where such information relates directly to the criminal predicate which is the basis for focusing on the individual or group.

Criminal Offender Record Information (CORI) defined in California Penal Code Section 11075(3) shall not be included in the intelligence file.

D. Criminal Intelligence File Criteria

All information retained in the Criminal Intelligence System must meet the criteria designated by the Sheriff. The criminal intelligence criteria includes data relating **only to the criminal activities** of individuals, organizations or groups.

E. Criminal Intelligence File System

Entries:

1. Any evaluated information which contains reasonable suspicion that an individual, organization, business, or group is suspected of being or having been involved in the actual or attempted planning, organizing, threatening, financing, or commission of criminal acts.

2. Any subject or entity to be entered shall be identifiable, distinguished by name and unique identifiers (e.g., DOB, CII number, driver's license number)

F. Information Evaluation

All new data received for filing consideration must undergo a review by the EOB Sergeant. Circulating information that has not been evaluated, where the source reliability is poor, or the content validity is doubtful, would be detrimental to the Department's operation and violates the individual's right to privacy. Evaluation of information is principally based upon the following:

Is it crime related?
Is it mission related?
Is it verified?

These considerations can be achieved by reviewing the newly arrived material. When the material passes this review, it will be classified for source reliability and content validity. Reliability and validity is classified using the following criteria:

I. Source reliability

I. **Reliable** - The reliability of the source is unquestioned or has been well tested in the past.

II. **Usually reliable** - The reliability of the source can usually be relied upon as factual. The majority of information provided in the past has proved to be reliable.

III. **Unreliable** - The source has been determined to be unreliable.

IV. **Unknown** - The reliability of the source cannot be judged. Its authenticity or trustworthiness has not yet been determined.

2. Content Validity

I. **Confirmed** - The information has been corroborated by an investigator or

another independent, reliable source.

II. **Probable** - The information is consistent with past accounts and is possibly true.

III. **Improbable** - The information is inconsistent with past accounts.

IV. **Cannot be judged** - The information cannot be judged. Its authenticity has not been determined by either experience or investigation.

G. Information Classification

Criminal Intelligence files should be classified to indicate the degree to which it is restricted in order to protect sources, to open investigations, and to ensure the individual's right to privacy.

1. **Sensitive** - Highest possible security. Access limited to those whose names appear upon the cover sheet.

2. **Confidential** - Medium level security. Access limited to intelligence personnel only.

3. **Restricted** - Lowest level of security. Access limited to law enforcement personnel only.

4. **Unclassified** - Public Information

H. Information Quality Control

Information to be stored in the Criminal Intelligence System must undergo a thorough review by the EOB Sergeant for compliance with system input guidelines and policy prior to being entered into the system. Both the originating employee and the EOB Sergeant are required to initial and date the Intake Report.

I. Source Identification

All criminal intelligence stored in the system must reflect the names of individuals and agencies that provided the original intelligence to the extent that it is appropriate and allowed under the law. In cases where the source is a confidential informant, only the C/I number, as assigned by the EOB Sergeant will be utilized. A cross referenced index system matching confidential informants to their respective numbers will be maintained by the EOB Sergeant.

J. File Dissemination

Information from a criminal intelligence report can only be released to an individual who has demonstrated both a "Need to Know" and a "Right to

Know".

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

"Right to Know" - Requestor has official capacity and statutory authority to the intelligence being requested.

No "original document" which has been obtained from an outside agency is to be released to a third agency. Should such a request be received, the requesting agency will be referred to the submitting agency for further assistance. Once it has been determined that the requestor meets the required criteria, criminal intelligence reports may be released under the following guidelines:

1. Criminal Intelligence reports classified as **Sensitive** can ***only*** be released with the approval of the EOB Lieutenant.

2. Criminal Intelligence reports classified as **Confidential** can be released with the approval of the EOB Lieutenant.

3. Criminal Intelligence reports classified as **Restricted** can be released with the approval of the EOB Sergeant.

4. **Unclassified** criminal intelligence reports can be released with the approval of an EOB Investigator.

Any information pertaining to a specific criminal intelligence case which has been authorized for release or dissemination should be released by the investigator who generated the information or is otherwise assigned to the case. Every effort should be made to notify the handling investigator of the intent to release information pertaining to his/her assigned case prior to the dissemination. The EOB Lieutenant shall make the final decision as to whether or not information will be released or otherwise disseminated in the absence of the assigned investigator.

Any time information from a criminal intelligence report is disseminated the release of intelligence must have an accessible audit trail. Release of any intelligence shall be documented through the use of the Criminal Intelligence Dissemination Form.

When disseminating criminal intelligence to any agency or individual, only information from the narrative is to be issued. Copies of the Intake Report or Intelligence Report shall not be disseminated.

Disclosure to the public of any information contained in the Criminal Intelligence System shall be done in accordance with the law. Under the California Public Records Act, Calif. Govt. Code 6254 (f) intelligence reports are confidential and are exempt from disclosure to the public.

K. Criminal Intelligence System Review and Purge

Intelligence stored in the system is to be audited on a quarterly basis for potential reclassification or purge. This quarterly audit is to ensure that all stored materials are accurate, relevant, timely and complete. The quarterly review will be supplemented by a daily review of the automated files by the Intelligence Analyst for purge dates (five year period) 30-60 days in the future. Each file nearing its purge date will be reviewed by the EOB Sergeant for either updating or a purge recommendation. When a file is found to lack one or more of the four following essential qualities and the quality of the information cannot be improved, the file then becomes subject to purge and deletion.

1. Purge Criteria Defined:

   a. **Accurate:** Verifications have been made by staff confirming that the details in the file are complete.

   b. **Relevant:** Proof exists that materials contained within the file meet intelligence report criteria.

   c. **Timely:** Filed materials relate to current unit crime interest.

   d. **Complete:** All facts and details are in file to support what is written in source documents.

When an audit determines that a criminal intelligence report is lacking one or more of these qualities, steps are taken to either upgrade or remove the report from file. Per the standards of federal and state criminal intelligence guidelines, all criminal intelligence reports may be retained for a period of five years and must subsequently be destroyed unless updated information indicates continuing criminal activity. It is therefore incumbent upon the EOB members to closely review any criminal intelligence report that indicates no activity for a period of five years.

2. Purging Procedures.

   Purging reports at five years of age or as soon as they are determined to lack "reliability".

When it has been determined that a criminal intelligence report meets the criteria outlined above for purging and falls within the guidelines for destruction, the EOB Sergeant shall collect all the information contained in the electronic file, complete a purge report and present it to the EOB Lieutenant for review prior to the actual purging.

It then becomes the responsibility of the EOB Lieutenant to determine whether to authorize the purging and deletion of the particular intelligence file by signing and dating the accompanying purge form. If authorization is granted, the entire report and purge form is returned to the originating EOB member who will be responsible for purging the record from the system. The purge form is to be maintained as proof that the file has been purged for authorized reasons.

L. Security

Confidential materials will be maintained in an area that has solid walls, floor, ceiling, and a solid core, restricted access door. All confidential criminal intelligence materials that are not computerized are to be stored in the designated criminal intelligence file room. The criminal intelligence system is a "stand-alone" computerized system, password and firewall protected, encrypted and physically secure.

Any individuals who breach, assist or attempt to breach the security of the Criminal Intelligence System will be subject to the appropriate penalty, sanction or discipline.

M. Criminal Intelligence System index and forms used.

The following is a description of the index and forms used by the Emergency Operations Bureau contained within the Criminal Intelligence System. Due to the nature of the EOB and material involved, the specific forms and reports are utilized only by the EOB.

Index File By Name and Address

A computerized indexing system that includes names, case numbers, personal identifiers, physical descriptors and last known addresses. Also included, when known, are such items as monikers, associates, vehicles, major crime categories, associated entities and other special entries such as scars, tattoos, etc. This file additionally identifies all reports on the listed subject, both by number and resume.

Criminal Intelligence Intake Report

The Intake Report identifies the criminal intelligence report, the type of document and indicates the information classification. The intake report will additionally depict whether the report is temporary or permanent and the date so designated. This designation is made by the Intelligence Sergeant with concurrence of the EOB Lieutenant.

Criminal Intelligence Report

The face sheet gives a brief synopsis of the report itself. It is this form that identifies the source(s) of each report; either by name or Confidential Informant number. It also contains a source reliability rating and information validity rating.

Criminal Intelligence Report - Narrative

The narrative portion must be constructed with no information that would indicate the origin of the report. It contains a narrative description of the information obtained.

Dissemination Form

This control form is used to record the date of a request, the name of the agency/individual requesting said information, the type of information released, the report's page/paragraph, and the name of the Officer handling the request.

Purge Form

The purge form is used to accompany any report taken from the file for consideration or purging and deletion. The form enables the EOB member to provide a brief explanation as to the perceived need for purging and deletion. The purge form provides a space for the EOB Sergeant and EOB Lieutenant to date and sign should they agree with the purge/deletion request. It is only when this form is complete and signed that a purge/deletion is authorized. Once the complete file is deleted, the purge form is maintained in hard copy where it serves as proof that the file has been purged for authorized reasons.

II. AUDIT OF INTELLIGENCE FILES

The EOB Lieutenant shall conduct periodic reviews on a random basis, but no less than quarterly of the Criminal Intelligence System to ensure compliance with Department guidelines.

III. CROSS-REFERENCE

Section 34090 of the California Government Code.
Code of Federal Regulations Article 28 Section 23
Olmstead vs. U.S. (1928) 277 U.S. 438.
Griswold vs. Connecticut (1965) 381 U.S. 479.
A.C.L.U. vs. Deukmejian (1982) 32 Cal.3d 440.
South Coast Newspapers, Inc., vs. Ocean Side (1984) 160 Cal. app. 3d
Williams vs. Superior Court (1993) 5c 4th 337.

Federal Freedom of Information Act, 5 U.S.C./552.
Federal Privacy Act, 5 U.S.C./552.
California Information Practices Act, C.C. Section 1798, et seq.
California Public Records Act, G.C. Section 6250 et seq.