SAN DIEGO POLICE DEPARTMENT
PROCEDURE

DATE:	March 29, 2013
NUMBER:	3.30 - INVESTIGATIONS
SUBJECT:	POLICE DEPARTMENT INTELLIGENCE SYSTEM (PDIS)
RELATED POLICY:	N/A
ORIGINATING DIVISION:	CRIMINAL INTELLIGENCE UNIT
NEW PROCEDURE:	☐
PROCEDURAL CHANGE:	■
SUPERSEDES:	05/28/2010

I. PURPOSE

A. This Department procedure establishes the guidelines for the implementation and utilization of the Police Department Intelligence System (PDIS). This application is designed to provide the San Diego Police Department (SDPD) with an effective and accessible intelligence system for the timely sharing of criminal intelligence information amongst all Department personnel.

B. The PDIS provides a computerized mechanism for the analysis of organized crime and criminal enterprises in San Diego, as well as assisting with the identification and/or projection of major changes in crime trends that may require adjustments in staffing and resource allocation.

C. The objectives of the PDIS are to prevent and control crime, while conforming to the privacy and constitutional rights of groups and individuals. The goals of the PDIS are to provide liaison, coordination and resource assistance in the collection, storage, exchange or dissemination, and analysis of criminal intelligence information in ongoing investigations or prosecution activities relating to specific areas of criminal activity.

D. The PDIS is also designed to provide criminal intelligence information to the appropriate investigative units on individuals involved with identified criminal organizations and enterprises.

II. SCOPE

A. This procedure applies to all members of the Department. The PDIS is managed and maintained by the San Diego Police Department's Criminal Intelligence Unit (CIU). Specific aspects of this procedure apply solely to CIU.

B. This procedure shall govern all intelligence systems operated and utilized by the San Diego Police Department and the release or distribution of intelligence information.

III. BACKGROUND

A. It is recognized that certain criminal activities often involve some degree of regular coordination and permanent organization involving a large number of participants over a broad geographical area.

B. 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.

C. Code of Federal Regulations

1. Title 28, Code of Federal Regulations, Part 23 (28 CFR 23) is a guideline for law enforcement agencies and contains implementation standards for operating federally grant-funded criminal intelligence systems. 28 CFR 23 was issued in 1980 to ensure the privacy and constitutional rights of individuals during the collection and exchange of criminal intelligence information and it has since been an important part of the intelligence landscape.

2. 28 CFR 23 specifically provides guidance in five primary areas:

    a. Submission and entry of criminal intelligence information;

    b. Security;

    c. Inquiry;

    d. Dissemination; and,

    e. Review-and-purge process.

3. The purpose of this regulation is to assure that all criminal intelligence systems are utilized in conformance with the privacy and constitutional rights of individuals.

4. The areas of criminal activity for which intelligence information is to be utilized represent a significant and recognized threat to the population, and are:

   a. Undertaken for the purpose of seeking illegal power and profits, or pose a threat to the life and property of citizens;

   b. Involve a significant degree of permanent criminal organization; or,

   c. Not limited to one jurisdiction.

5. 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.

IV. DEFINITIONS

A. Criminal activity - any activity that violates state statutes, ordinances, or codes, and constitutes a criminal act under the law (excluding traffic violations).

B. Criminal associate - an individual who is suspected of maintaining criminal associations and involvement with any individual, group, or organization reasonably suspected of engaging in criminal activity.

C. Criminal intelligence information - data that has been evaluated to determine that it is relevant to the identification of, and the criminal activity engaged in, by an individual or organization reasonably suspected of involvement in criminal activity, and meets PDIS submission criteria.

D. Criminal intelligence system or intelligence system - the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information.

E. Intelligence project - the organizational unit that operates an intelligence system on behalf, and for the benefit, of a single agency or the organization that operates an inter-jurisdictional intelligence system on behalf of a group of participating agencies.

F. Jurisdictional boundaries - the area within any city or county within the area served by the PDIS.

G. Modus Operandi - a unique method of operation for a specific type of crime and may not be immediately linked to an identifiable suspect.

H. Need-to-know - the necessity to obtain or receive criminal intelligence information in the performance of official responsibilities as a law enforcement or criminal justice authority.

I. Organized crime - any organized group that has its leadership insulated from direct involvement in criminal acts and ensures organizational integrity in the event of a loss of leadership.

J. Reasonable suspicion or criminal predicate - 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 there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise.

K. Right-to-know - the right to obtain or receive criminal intelligence information because of his or her status as a sworn member of a law enforcement agency in accordance with a specific law enforcement purpose or pursuant to a court order or statute.

L. Traveling criminals - individuals, groups, or organizations engaged in or otherwise associated with criminal activity that traverses jurisdictional boundaries.

M. Validation of information - 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.

V. PROCEDURES

A. The PDIS is focused on compiling, storing and disseminating criminal intelligence information on individuals and organizations involved with significant criminal activities.

B. Submission Criteria and Data

1. CIU personnel, or their designee, shall train Department personnel relating to the nature, scope and capabilities of the PDIS application. This training session is required PRIOR to Department personnel utilizing the PDIS application.

2. Upon completing the required training, the Department member will complete the PDIS Access Form. The completed form will be utilized by the PDIS staff to add the Department member as an authorized user. The PDIS Access Form template is contained on the last page of this procedure.

3. SDPD personnel shall only collect and maintain criminal intelligence information concerning an individual 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.

4. **SDPD personnel 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.**

5. CIU is ultimately responsible for establishing the existence of reasonable suspicion of criminal activity through examination of supporting information submitted by Department personnel.

6. **SDPD personnel shall not include in the PDIS any information that has been obtained in violation of any applicable federal, state, or local law or ordinance. CIU is responsible for ensuring that no information is entered in the PDIS in violation of federal, state, or local laws through examination of supporting information submitted by all Department personnel.**

7. CIU can reject or request corrections on PDIS entries made by Department personnel.

8. PDIS Data Entry

    a) Subject Identification

        Subjects should be identified by unique identifying characteristics. The more specific identifying information about the subjects of the intelligence reports, the more useful the information is to investigators.

    b) Sources of information can include any of the following:

        (1) Information Source

(a) Anonymous

(b) Arrest

(c) Concerned Citizen

(d) Field Interview

(e) Investigative Interview

(f) Open Source

(g) Other Agency

(h) Personal Observation

(2) Confidential Informant (CI)

Names or identifying information of informants or cooperating witnesses will not be used in this database. At the investigators discretion the investigator may use the CI reference number if the classification is at a high level.

(3) Source Reliability (Refer to Section V.C., Labeling Information)

(a) Reliable

(b) Usually Reliable

(c) Unreliable

(d) Unknown

(4) Content Validity (Refer to Section V.C., Labeling Information)

(a) Confirmed

(b) Probable

(c) Doubtful

(d) Cannot be Judged

(5) Location

(6) Division

(7) Beat

(8) Information Classification (This level of security will vary depending on the nature of the type and source of the information.)

(9) Gang Name (See dropdown menu for appropriate selection)

(10) Crime Type (up to five crime type categories can be selected)

(11) Entry Status

(a) Permanent

(b) Temporary

(12) Gang-related

(13) Division Specific

(14) The following submission information will be recorded automatically by the PDIS application:

(a) Date of Submittal of Information

(b) Submitting Officer's Name

(c) Name of Submitting Command

(15) Information from open source and law enforcement bulletins and publications.

(a) All information derived from either open source or law enforcement bulletins, publications or documents shall be forwarded to CIU for submission in the PDIS application.

(b) Information and bulletins should not be distributed Department-wide without the consent of the Chief of Police, or his designee.

9. Prohibited Information

a. Based on the sensitive nature of certain investigations, the names or other specific indentifying information of confidential informants shall never be entered in the PDIS application.

b. When entering information developed through a confidential informant or cooperating witness only their control number or the word “source” will be used.

C. Labeling of Information

1. Information to be retained in the PDIS shall be labeled for source reliability and content validity prior to entry or submission.

a. Source Reliability

(1) The reliability of the source is an index of the consistency of the information the source provide.

(2) The source of the information shall be evaluated using the following criteria:

(a) Reliable – the reliability of the source is unquestioned or has been well tested in the past.

(b) Usually Reliable – the reliability of the source can usually be relied upon. The majority of the information provided in the past has proved to be reliable.

(c) Unreliable – the reliability of the source has been sporadic in the past.

(d) Unknown – the reliability of the source cannot be judged; authenticity or trustworthiness has not yet been determined by either experience or investigation.

b. Content Validity

(1) The validity of information is an index of the accuracy or truth of the information. The validity of the information shall be assessed as follows:

(a) Confirmed – the information has been corroborated by an investigator or another reliable independent source.

(b) Probable – the information is consistent with past accounts.

(c) Doubtful – the information is inconsistent with past accounts.

(d) Cannot Be Judged – the information cannot be judged. Its authenticity has not yet been determined by either experience or investigation.

2. Information maintained in the PDIS may be labeled using any combination of the above Source Reliability and Content Validity designations, except for the combination of "Unknown" for Source Reliability and "Cannot Be Judged" for Content Validity—this particular combination does not meet reasonable suspicion criteria and will be rejected from inclusion in the PDIS database.

D. Inquiry Procedures

1. Inquiries can be made without reasonable suspicion of criminal activity as long as the person requesting the information has a right-to-know and a need-to-know for a specific law enforcement purpose.

2. Any authorized SDPD member may initiate an inquiry to the PDIS, but information will be disseminated only to designated personnel who have authorized access.

3. Any authorized outside agency member may initiate an inquiry to the PDIS directly through CIU. Information can only be released to other agencies by CIU.

4. Prior to dissemination of information, the identity of the inquiring officer must be confirmed. If access is by telephone, mail, e-mail, or facsimile, CIU may use a personal data sheet or security control card maintained on file. In this instance, release of information shall be made on a call-back basis only after verification of the identity of the officer.

5. All inquiries of the PDIS will be conducted through the database Filter and Search menu.

E. File Criteria

1. Permanent File

a. Organizations

(1) Any organized criminal group.

(2) Any organizations that threaten, attempt, plan or perform acts of terrorism, or perform unlawful acts disruptive of the public order, or who perform other criminal acts.

(3) Organizations that are suspected of being operated, controlled, financed or infiltrated by known or suspected crime figures for use in an illegal manner.

(4) Gangs involved in any illegal activities.

(5) Organizations whose primary purpose is sustaining or financing criminal organizations.

b. Individuals

(1) Any individual who is reasonably suspected of being a member of any criminal gang or organization, or who is reasonably suspected of being involved with known crime figures and a criminal predicate exists.

(2) Any individual who threatens, attempts, plans or performs any act of terrorism.

(3) Any individual who is reasonably suspected to be planning, encouraging, advising, or preparing the commission of a criminal act, or who is reasonably suspected to have been a principal or accessory in the commission of a criminal act.

(a) In addition to falling within the confines of one or more of the above criminal activities, the individual to be entered into the permanent intelligence file database should be identifiable and distinguished by a unique identifying characteristic (i.e. date of birth, criminal identification number, driver's license number, etc.)

(b) Identification at the time of file input is necessary to distinguish the subject from any similar person in the database or any others that may be entered at a later time.

(4) Any individual who is reasonably suspected of criminal activity which demonstrates sophistication, organization or repetitive patterns that needs analysis.

c. Criminal Activity

(1) Any criminal activity which demonstrates sophistication, organization or repetitive patterns that needs analysis.

2. Temporary File

a. Under some circumstances it is desirable to maintain information on an individual or organization on a temporary basis although it does not meet the criteria for entry into the PDIS. This information should be separately maintained and should not be made part of the PDIS until it satisfies the entry criteria.

b. Following are examples of reasons information would be gathered and maintained on a temporary basis:

(1) The subject is unidentifiable, although reasonably suspected to be engaged in criminal activities, has no physical descriptors, identification numbers, or distinguishing characteristics available.

(2) The subject's level of involvement is questionable; however, based on one of the following it would be beneficial to the agency to retain a record of the subject for a limited period of time during which the information can be validated;

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

(b) Criminal history - the individual or organization, although not currently reported to be criminally active, has a history or criminal conduct, and the circumstances currently being reported, i.e., new position or ownership in a business, affords an opportunity to again become criminally active.

(c) The information's reliability/validity is unknown - the reliability of the information source and/or the

validity of the information content cannot be determined at the time of receipt; however, the information appears to be significant and merits temporary storage while verification attempts are made.

c. The separately maintained, temporary files should be actively "worked" in an effort to determine whether it meets the necessary criteria to either be added to the intelligence system or be destroyed. Persistent efforts should be made to identify the subject or further validate the information so that its final status may be determined.

d. The temporary file and all of the information collected shall be purged within 90 days from the date of entry if there is no compelling reason for its retention. The reason shall be thoroughly documented as to why the information deserves retention as a temporary file.

3. Material stored in the PDIS database should be restricted to documents of criminal intelligence, and related information from public records and media sources. Criminal Offender Record Information (CORI) and information not meeting the criteria for file input should be excluded from storage in the criminal intelligence file.

4. **Examples of excluded material are religious, political, or sexual information which does not relate to criminal conduct and associations with individuals which may not be of a criminal nature.**

F. Access Rights

1. Restrictions on release of the information based on the designated dissemination level are always established and enforced by CIU with the exception that a contributor of information may view the data he or she submitted regardless of the designated dissemination level.

2. For system administration and maintenance purposes, specific members of CIU may have access to all information regardless of the dissemination level.

3. Only the Primary Representative or designee in CIU may distribute information to an outside law enforcement agency.

4. When providing information to an outside law enforcement agency, the Primary Representative or designee in CIU will establish the need for the access to the PDIS record and to what extent.

5. Telephone, e-mail, and facsimile requests for criminal intelligence information will be addressed only after the requester's authorization is determined.

6. Intelligence information and intelligence may never be released to civilian personnel except by court order and with the authorization of the CIU lieutenant.

7. CIU reserves the right to deny PDIS access.

G. Dissemination of Information

1. Dissemination Procedures

a. CIU personnel shall disseminate criminal intelligence information only where there is a valid need-to-know and a right-to-know the information in the performance of a specific law enforcement activity.

b. CIU shall disseminate criminal intelligence information only to law enforcement or criminal investigative authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination that are consistent with these operating policies and procedures.

c. This procedure 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.

d. The 'Third Agency Rule' is an information-sharing restriction.

(1) If a Department member receives case intelligence from an intelligence source (such as a fusion center), that officer cannot disseminate the intelligence to a third party without permission from the original source.

(2) CIU will coordinate with the outside agencies to facilitate appropriate information sharing in compliance with the 'Third Agency Rule.'

2. Dissemination Level

The dissemination level is the classification of information and how it is to be shared within the San Diego Police Department, as well as with other

law enforcement agencies. CIU is responsible for the dissemination of all intelligence information.

3. Dissemination Record

a. An audit trail or dissemination record is required when information is disseminated from the PDIS application.

b. The record shall contain the following information:

(1) Date of dissemination of the information;

(2) Name of the individual requesting the information;

(3) Name of the agency requesting the information;

(4) Reason for the release of the information (need-to-know/right-to-know);

(5) Information provided to the requester;

(6) Name of CIU member disseminating the information; and,

(7) CIU personnel disseminating information shall maintain an audit trail/dissemination record

H. Review and Purge

1. Purge Procedures

a. Reviewing and purging information in the PDIS should be done on an ongoing basis by CIU personnel.

b. The maximum retention period is five years, unless a continuing criminal predicate exists that can be clearly articulated and is connected to current activity. If the information has not been updated and/or validated, it must be removed from the system at the end of the retention period.

c. The submitting personnel may update and/or validate the submission and extend the retention period at any time.

d. The review, validation, and purge process may be a manual process, or an automated process, or a combination of both.

e. A data field is required so that a determination can be made of how long the information has been in the PDIS and when it is due for purging.

f. Purge dates are initially calculated based on the submittal date and the submittal type and can be generated automatically, or the purge date could be manually entered. If a purge date is modified, then all links to the records must be evaluated and modified appropriately.

g. CIU may adopt a policy to purge information without notification to the submitting personnel or adopt a policy to notify the submitting personnel prior to purge of information to provide the submitting person an opportunity to validate the submission and extend the retention period.

h. The process adopted should not delay the purging of information that has reached the end of its retention period (i.e., information may not remain in the database longer than the retention period without validation and updating.)

i. If there has been no update or re-submission of the information by the submitting Department member, then it is automatically purged at the end of the five-year period.

2. Purge Notifications

a. Once a month CIU will develop a list of their submissions scheduled to be purged within the next 90 days.

b. If CIU chooses to retain a submission, it must be validated by a pre-designated CIU officer. Failure to review and validate the submission will result in the submission being purged.

c. CIU, or a CIU designee conducting the review, shall make a determination that some or all of the information contained in the submission continues to comply with 28 CFR 23 requirements.

d. Information concerning each individual, group, association, corporation, business, or partnership named in the submission shall be reviewed to determine if that individual, group, association, corporation, business, or partnership continues to be reasonably suspected of being involved in the criminal activity described in the submission.

e. If this determination is made, the primary representative from CIU or the designee can extend the retention period.

f. All information retained as a result of this review shall reflect the name of the reviewer, date of review, and explanation of decision to retain.

g. If this cannot be established, the name of the individual, group, association, corporation, business, or partnership will be deleted from the database.

h. Any information that is found to be misleading, obsolete, or otherwise unreliable will be purged on an ongoing basis by CIU.

3. Destruction of Files

b) Material purged from the PDIS will be returned to the submitting personnel by CIU or confidentially destroyed.

c) Department personnel shall not keep personal or private intelligence files separate from the PDIS database.

d) Only an administrative record of the purge will be maintained. No record of the names of individuals, organizations, etc., that are purged will be maintained by CIU.

I. Inspection and Audit of Files

1. The PDIS application will automatically create a record, which will serve as an audit trail, each time a user accesses the PDIS database for any purpose including entries, inquires, or any other function.

2. CIU will periodically conduct audits and inspections of the records that support submissions to the PDIS database and compliance with operating principles set forth in 28 CFR Section 23.20, with regard to submissions made to the PDIS.

J. Security of PDIS Files

1. In order to maintain the confidentiality of stored criminal intelligence information and to ensure the protection of the individual's right to privacy, the Commanding Officer of CIU, or the designee, shall be responsible for implementing the following security requirements for the PDIS:

a. The PDIS database shall be located in a physically secured area that is restricted to designated authorized personnel.

b. When it becomes necessary for staff to access the server or the database, CIU personnel will be physically present.

c. Only designated authorized personnel will have access to information stored in the PDIS database.

d. All hardcopy submissions and/or manual files will be secured by San Diego Police Department personnel when not being used and at the end of each shift.

e. No printed intelligence information will be left in an area where unauthorized persons can access or read the documents.

f. Employment policies and procedures for screening/rejecting, transferring, or removing personnel having direct access to the PDIS will be controlled by CIU. The Commanding Officer of CIU reserves the right to suspend PDIS access rights to any personnel without notice.

g. The data contained in the PIDS will be encrypted and the most recent technology will be utilized to protect the database.

PDIS Access Form

To be completed by user:

Username: _____

First Name: _____

Last Name: _____

Title: _____

Division: _____

Commanding Officer: _____

E-mail: _____

To be completed by CIU or PDIS Staff:

Command Chain Level: _____

Security Level: _____

- ❑ **Active**
- ❑ **Admin**
- ❑ **Trigger Admin**
- ❑ **Classification Modifier**
- ❑ **Intel Approver**