CALIFORNIA HIGHWAY PATROL

GENERAL ORDER 81.6

REVISED OCTOBER 2019

INVESTIGATIVE INFORMATIONAL DATABASE SYSTEMS

1. PURPOSE.

   a. The purpose of this General Order (GO) is to establish policy and procedures for all departmental personnel relative to the use of investigative informational databases. This will include the identification, authorization, implementation, and proper utilization of these systems in order to assist in departmental investigations.

   b. The purpose of investigative informational databases is to provide a technologically advanced means for departmental personnel to gather automated information relative to criminal investigations and enforcement contacts.

2. GENERAL.

   a. With the creation of databases to gather and maintain information, it has become necessary for the Department to secure access to these investigative databases in order to assist with departmental investigations. Historically, law enforcement has utilized the National Crime Information Center (NCIC) and the California Law Enforcement Telecommunications System (CLETS) to obtain viable information to assist in investigations. Today, these systems continue to play a significant role in providing law enforcement with much needed criminal information. However, there are a number of innovative investigative information systems available for use by law enforcement. Some of these systems include the El Paso Intelligence Center Network (EPIC), the National Insurance Crime Bureau (NICB), the California Department of Corrections and Rehabilitation (CDCR) - Parole Law Enforcement Automated Database System (Parole LEADS), Public Records Information (PRI) Database, Western States Information Network (WSIN)/Regional Information Sharing System (RISS), the Department of Justice (DOJ) California Photo Mugshot Program (Cal-Photo), the DOJ Automated Archive System (AAS), and the International Criminal Police Organization (INTERPOL).

   b. Enforcement and Planning Division (EPD), Field Support Section (FSS), has been assigned Office of Primary Interest (OPI) responsibility for the identification, authorization, and implementation of investigative informational databases. As the OPI for investigative informational databases, FSS acts as departmental liaison to

system providers, and maintains administrative control in matters regarding access to investigative informational database systems by departmental users.

3. POLICY. The content of this GO establishes policy which governs the overall administration and operation of investigative informational databases utilized by the California Highway Patrol (CHP).

4. RESPONSIBILITIES.

a. Assistant Commissioner, Staff. Under the direction of the Commissioner, the Assistant Commissioner, Staff (ACS), exercises overall operational control of investigative informational databases. All policy changes relative to investigative informational databases shall be approved by ACS prior to implementation. Additionally, EPD and Information Management Division will assist ACS by providing recommendations relative to investigative informational databases.

b. Enforcement and Planning Division. Under the direction of ACS, and with the assistance of FSS, EPD provides recommendations and advice to members of Executive Management regarding the management and administration of investigative informational databases. Additionally, EPD coordinates with members of Top Management and assists ACS with management and oversight of investigative informational databases. Enforcement and Planning Division participates in the decision-making process regarding technical and operational issues relative to investigative informational databases. Further, EPD develops policies, procedures, and objectives with regard to the databases.

c. Field Support Section. Under the direction of EPD, FSS is the facilitator and liaison to ACS for all field Divisions. Field Support Section advises EPD on all matters related to investigative informational databases. Furthermore, FSS provides advice and assistance to field Divisions and Area offices regarding the administration, management, and utilization of these databases. Field Support Section personnel provide input regarding user identification, provide or arrange training for all users, and identify potentially viable investigative databases.

d. Information Management Division. Information Management Division is responsible for working with EPD to provide recommendations and advice relative to network compatibility.

e. Information Security Officer. The Information Security Officer (ISO) approves network access for nondepartmental employees (Highway Patrol Manual [HPM] 40.4, Information Security and Administration Manual, Chapter 7, Information Systems Account Management Policy). The ISO also has responsibility for determining when security incidents are subject to Section 1798.29 of the Civil

Code (relating to privacy data) and working with commands to make necessary notifications. It is the responsibility of every employee to ensure privacy data (California driver license, Social Security number, and certain financial data) is properly safeguarded. In the event any of this data is lost, stolen, or accessed by an unauthorized person, the ISO shall be immediately notified (HPM 40.4, Chapter 1, General). The ISO is also to be notified in the event of lost or stolen state-owned equipment (HPM 40.4, Chapter 1).

f. Information Technology Security Reporting Requirements are elaborated in HPM 40.4, Chapter 1.

g. Departmental employees requesting access to specific data processing resources shall submit a CHP 109, Information Technology Request, signed by their commander.

h. The responsibility of every employee and commander for securing confidential and privacy information is discussed in HPM 40.4, Chapter 1.

i. Field Divisions and Protective Services Division. Field Divisions and Protective Services Division (PSD) Chiefs exercise overall control of their personnel authorized to utilize investigative informational databases within their respective Divisions. It is the responsibility of the Division Chief to ensure Division personnel are in compliance with policies and procedures contained within this GO. Additionally, Division Chiefs should consult with EPD regarding operational issues related to investigative databases. Issues requiring policy changes or matters that cannot be resolved by direct coordination between field Divisions and EPD shall be referred by EPD, through channels, to the appropriate Commissioner for direction.

j. Division Investigative Services Unit Coordinators. Division Investigative Services Unit (ISU) coordinators, in conjunction with their respective Division training coordinators, are responsible for the administration and operation of all investigative informational databases within their Division. The ISU coordinator may identify a designee from the ISU to act as the liaison to FSS and Area offices. The Division ISU coordinator or designee shall be responsible for the facilitation and coordination of training related to investigative informational databases. For those investigative databases not available to Areas, the ISU coordinator or designee will be responsible for providing investigative assistance, as necessary.

k. Area Accountability. The Area commander or designee is responsible for ensuring Area personnel authorized to utilize investigative informational databases comply with the policies and procedures as outlined in this GO.

5. AUTHORIZATION. Departmental personnel seeking authorization to access an investigative informational database shall follow the access instructions for the specific database as required in paragraph 6. of this GO.

6. INVESTIGATIVE INFORMATIONAL DATABASE SYSTEMS.

a. Investigative informational database systems play a valuable role in the way law enforcement agencies investigate criminal activity. Due to the sensitive and confidential nature of the information within these systems, a number of databases have been deemed right-to-know and need-to-know access only. Pursuant to policy established in HPM 40.4, departmental employees/computer users are responsible for protecting the Department's information technology assets. Employees shall ensure access is only requested commensurate with each employee's job duties and responsibilities.

(1) Right-to-know: requestor has the right to obtain information pursuant to a court order, statute, or decisional order.

(2) Need-to-know: requestor has the need to obtain information in order to execute official responsibilities.

NOTE: Informational database entries are to be consistent with the guidelines established in Title 28, Code of Federal Regulations, Part 23 (Annex A). All information entered is discoverable under the California Public Records Act and must be professional in nature, as well as in compliance with applicable laws and departmental policies.

b. Authorization to utilize these systems necessitates the approval of the respective Division, and for NICB, PRI, and AAS systems, FSS approval. Upon authorization, the following investigative informational databases have been approved by the Commissioner for access and use by departmental personnel:

(1) El Paso Intelligence Center Network.

(a) Background. The EPIC is a unique, cooperative effort established to collect, process, and disseminate intelligence information concerning illicit drugs and currency movement, alien smuggling, weapons trafficking, and related activity. It is staffed by personnel from state agencies and 15 federal agencies, and coordinated by the United States Drug Enforcement Administration.

(b) Database Information. The EPIC maintains an automated criminal intelligence index which provides all member agencies with quick access to accurate and timely intelligence information on interstate and international drug traffickers. The EPIC maintains four separate and

unique database systems. The following systems are available through EPIC:

1 Internal Database System.

2 Narcotics and Dangerous Drugs and Information System.

3 Treasury Enforcement Communications System.

4 Integrated Combined System.

(c) Access.

1 The EPIC database is to be used as an investigative resource. Inquiries to the EPIC should be made only if the information to be gained is associated with one or more of the following areas: illegal drug smuggling/trafficking, alien smuggling, weapons trafficking, fugitives, stolen weapons, vehicles, aircraft, and vessels. Access is generally limited to personnel assigned to FSS, ISUs, drug task force members, PSD, and personnel assigned to other investigative duties. Uniformed personnel not authorized access, but who require information from the EPIC, may contact their Division ISU, local drug task force, or FSS.

2 Field Division and Area personnel requesting access must submit an e-mail to their respective Division ISU coordinator for approval. Field Support Section maintains a current roster of all personnel authorized access. Accordingly, FSS shall be notified as soon as possible by the Division ISU coordinator of anyone whose access to the system is no longer authorized.

(2) National Insurance Crime Bureau.

(a) Background. The NICB was established by insurance industry carriers to effectively assist law enforcement and the insurance industry in combating insurance fraud and vehicle theft activities nationwide.

(b) Database Information. The NICB allows authorized users to access the NICB database, which contains over 350 million records. The NICB provides information relative to insurance claims, manufacturers' shipping records, vehicle histories (including purged stolen vehicle records), and Vehicle Identification Number (VIN) locations for various manufacturers. This system is available to departmental personnel involved in vehicle theft investigations and the VIN replacement program.

(c) Access.

1 The NICB database is to be used as an investigative resource. Inquiries into NICB must be in relation to an ongoing criminal investigation or arrest. Access is generally limited to uniformed personnel assigned to ISUs, VIN officers, Salvage Vehicle Inspection officers, Area follow-up investigators, PSD, and personnel assigned to other investigative duties. Uniformed personnel not authorized access, but who require information from NICB, may contact their Area VIN officer, Division ISU, or FSS.

2 Field Division and Area personnel requesting access must submit an e-mail to their respective Division ISU coordinator for initial approval. Requests will then be forwarded to FSS for final approval. Individuals approved for access will be provided required training. Field Support Section maintains a current roster of all personnel authorized access. Accordingly, FSS shall be notified as soon as possible by the Division ISU coordinator of anyone whose access to the system is no longer authorized.

(3) Parole Law Enforcement Automated Data System.

(a) Background. The Parole LEADS allows California law enforcement agencies controlled and secure access of selected parolee information through the Internet.

(b) Database Information. The system allows authorized users to obtain parolee information in two ways from an extract of CDCR, Parole and Community Services Division, Statewide Parolee Database. Local agency users can either access information on a search query basis or request a database download consisting of the agency's group of parolee records updated since a user-selected date. The system allows the user to query the database via 48 different fields, ranging from name and date of birth to scars, marks, and tattoos.

(c) Access.

1 This system has been deemed a need-to-know, right-to-know system; therefore, personnel authorized to access Parole LEADS will be approved by their respective Divisions. Personnel authorized direct access will generally include those assigned criminal investigative duties. In addition, Divisions will ensure an appropriate number of communications center personnel are approved for access, in order to allow road patrol personnel to obtain system information via radio.

2 Field Division and Area personnel requesting access must submit an e-mail to their respective Division ISU coordinator for approval. Upon approval, end user agreements shall be filled out by the approved user and their respective Division coordinator, and forwarded to FSS. Parole LEADS personnel will be responsible for the training of Department personnel approved to access Parole LEADS. Field Support Section maintains a current roster of all personnel authorized access. Accordingly, FSS shall be notified as soon as possible by the Division ISU coordinator of anyone whose access to the system is no longer authorized.

(d) The California Values Act. Pursuant to California Government Code (GC) Title 1, Division 7, Chapter 17.25 (commencing with Section 7284), federal, state, or local law enforcement agencies shall not use any noncriminal history information contained within this database for immigration enforcement purposes. "Immigration enforcement" includes any and all efforts to investigate, enforce, or assist in the investigation or enforcement of any federal civil immigration law, and also includes any and all efforts to investigate, enforce, or assist in the investigation or enforcement of any federal criminal immigration law that penalizes a person's presence in, entry, or reentry to, or employment in, the United States (U.S.), as defined per Section 7284.4(f) GC. This restriction does not pertain to any information that is regarding a person's immigration or citizenship status pursuant to Title 8, U.S. Code Sections 1373 and 1644.

(4) Public Records Information Database System.

(a) Background. Current PRI technology allows access to over 1,600 public information databases throughout the country. Field Support Section contracts with one of the various commercial vendors that provide access to these databases.

(b) Database Information. The PRI database system is on a need-to-know, right-to-know basis. This system provides public information relative to Social Security numbers, bankruptcies, judgments, liens, real property ownership, corporations, and limited partnerships, as well as civil and criminal court docket scans. The system also includes a people locator feature. This is an invaluable tool to law enforcement because it provides a single source for gathering valuable information to assist in locating suspects and also provides crucial information for successful prosecutions.

(c) Access.

1 The PRI is to be used as an investigative resource. Inquiries into the PRI database must be in relation to an ongoing criminal investigation, arrest, or CHP uniformed and nonuniformed applicant background investigation. Access is generally limited to personnel assigned to ISUs, Area follow-up investigators, PSD, and personnel assigned to other investigative duties. Uniformed personnel not authorized access, but who require information from PRI, may contact their Area follow-up investigator, Division ISU, or FSS.

2 Field Division and Area personnel requesting access must submit an e-mail to their respective Division ISU coordinator for initial approval. Requests will then be forwarded to FSS for final approval. Field Support Section maintains a current roster of personnel authorized access. Accordingly, FSS shall be notified as soon as possible by the Division ISU coordinator of anyone whose access to the system is no longer authorized.

(d) Field Division and Area office inquiries can be made directly to FSS by telephone on a call-back basis, or by departmental e-mail. Field Support Section staff members who have completed required training may access the PRI database files. Information received from the PRI provider may be included in arrest/incident reports.

(5) Western States Information Network/Regional Information Sharing System.

(a) Background. The U.S. DOJ and the California State DOJ established WSIN in 1981. The geographical area covered by WSIN includes the states of California, Oregon, Washington, Alaska, and Hawaii. The mission of WSIN is to promote the exchange of intelligence information by providing necessary analytical support to identify criminal organizations, and to act as a central repository for the member states regarding information on criminal activity. In April of 1998, WSIN expanded its capabilities to interact with RISS, which is comprised of several regional systems throughout the U.S.

(b) Database Information. The RISS and WSIN are secure Intranet Web systems which create a network of intelligence information restricted to law enforcement use only. The WSIN maintains the Automated Criminal Intelligence Index, which provides its member agencies with quick access to accurate and timely intelligence information. This index offers searching capabilities that are possible only with an automated system. Regional Information Sharing System adds the capability of accessing similar regional databases from all over the country.

(c) Access.

1 The WSIN and RISS databases are to be used as a criminal investigative resource. Inquiries into these systems must be in relation to an ongoing investigation or arrest. Access is generally limited to personnel assigned to FSS, ISUs, drug task force members, PSD, and personnel assigned to other investigative duties. Uniformed personnel not authorized access, but who require information from WSIN and RISS, may contact their Division ISU, local drug task force, or FSS. Information received from these systems, after receiving confirmation from the submitting agency, may be included in arrest/incident reports.

2 Field Division and Area personnel requesting access must submit an e-mail to their respective Division ISU coordinator for approval. Field Support Section maintains a current roster of all personnel authorized access. Accordingly, FSS shall be notified as soon as possible by the Division ISU coordinator of anyone whose access to the system is no longer authorized.

(d) The California Values Act. Pursuant to GC Title 1, Division 7, Chapter 17.25 (commencing with Section 7284), federal, state, or local law enforcement agencies shall not use any noncriminal history information contained within this database for immigration enforcement purposes. "Immigration enforcement" includes any and all efforts to investigate, enforce, or assist in the investigation or enforcement of any federal civil immigration law, and also includes any and all efforts to investigate, enforce, or assist in the investigation or enforcement of any federal criminal immigration law that penalizes a person's presence in, entry, or reentry to, or employment in, the U.S., as defined per Section 7284.4(f) GC. This restriction does not pertain to any information that is regarding a person's immigration or citizenship status pursuant to Title 8, U.S. Code Sections 1373 and 1644.

(6) California Photo Mugshot and Department of Motor Vehicles Image System.

(a) Background. The DOJ maintains state summary criminal history information consisting of the master record of information on criminals compiled by the attorney general's office. That information includes names, aliases, dates of birth, physical descriptions, fingerprints, date(s) of arrest(s), charges, dispositions, and other pertinent data. The DOJ also maintains a secure, dedicated communication system, which makes the summary criminal history information available to all law enforcement agencies in the state via a uniform statewide communications network.

Law enforcement agencies throughout the state collect photographs of criminals, usually mugshots, and maintain them in various levels of automation. Many law enforcement agencies submit photos to DOJ pursuant to California's Megan's Law. The Cal-Photo and Department of Motor Vehicles (DMV) Image System allows for the electronic sharing of photos and DMV's 32 million images among and between law enforcement agencies.

(b) Database Information. The Cal-Photo is accessed from a personal computer's (PC) Web browser in a secure Intranet Web environment. California Photo Mugshot Program and DMV Image System conforms to National Institute of Standards and Technology (NIST) standards. The Cal-Photo utilizes the secure DOJ communication network and adheres to the CLETS Policies, Practices, and Procedures (PPP). Users of Cal-Photo must have DOJ network connectivity. Each county, city, and federal agency wishing access must submit an application and be approved for access by both DOJ and DMV. Each individual person wishing to access Cal-Photo must meet the security requirements and be authorized by their commander and Division Cal-Photo administrator. The Cal-Photo database provides access to mugshot images maintained by California's law enforcement agencies, as well as a connection to the photographs and data maintained by the California DMV. The Cal-Photo network and application are maintained by the DOJ Cal-Photo Program and the Hawkins Data Center within DOJ.

(c) Access.

1 Mugshots and DMV photo images are only accessible to Class I, II, and III law enforcement agency personnel as defined in Section 1.3.1 A, B, & C of the CLETS PPPs. A Class I law enforcement subscriber is defined as a governmental agency having statutory powers of arrest and whose primary functions are that of apprehension and detection. Class I subscribers include, but are not limited to, sheriff's departments, city police departments, CHP, DOJ, and the Federal Bureau of Investigation (FBI). The application for Cal-Photo access must be signed by the Commissioner and approved by DOJ and DMV before access will be granted. A new Cal-Photo User Agreement shall be updated at least every three years, when the head of the agency changes, or immediately upon request from the DOJ Cal-Photo Program.

2 Field Division and Area personnel requesting access must submit an e-mail to their respective Division ISU coordinator for approval. Field Support Section maintains a current roster of all personnel authorized access. Accordingly, FSS shall be notified as soon as

possible by the Division ISU coordinator of anyone whose access to the system is no longer authorized.

(d) Security. The Cal-Photo (which includes mugshots and DMV images) is considered Criminal Offender Record Information (CORI) and falls under CORI rules and statutes. All transactions are programmatically logged and subject to audit by the respective participating agencies, DOJ and DMV. All participants, nonuniformed and uniformed personnel, must be fingerprinted and have a fingerprint check response on file prior to being granted access to Cal-Photo. It is required that each employee having access to Cal-Photo sign the CLETS Employee/Volunteer Statement Form prior to operating or having access to Cal-Photo. These forms do not need to be completed if already on file as a result of departmental training procedures.

1 Additional requirements may be added at an agency's discretion. User identifications and passwords ensure access security. Each person wishing to access Cal-Photo must complete a New User Account and/or Administrator Account Form.

a These forms are available through DOJ Cal-Photo section and are to be maintained by each CHP Division's Cal-Photo administrator. Each person will assign their own user ID (6-10 characters) and passwords, which are case sensitive. A default password will be assigned by each CHP Cal-Photo Division administrator initially, but to ensure security, the password must be changed the first time the system is accessed and then shall be changed once every 90 days or less as desired by the user. After a password expires or has been changed, it shall not be used by the same person for at least four iterations. The Cal-Photo terminals and information must remain secure from unauthorized access. Access to information through Cal-Photo is on a right-to-know and need-to-know basis. Authorized personnel shall not inquire into their own record or have someone inquire for them. Accessing and/or releasing Cal-Photo information for non-law enforcement purposes is prohibited and is subject to administrative action and/or criminal prosecution.

(e) The California Values Act. Pursuant to GC Title 1, Division 7, Chapter 17.25 (commencing with Section 7284), federal, state, or local law enforcement agencies shall not use any noncriminal history information contained within this database for immigration enforcement purposes. "Immigration enforcement" includes any and all efforts to investigate, enforce, or assist in the investigation or enforcement of any federal civil immigration law, and also includes any and all efforts to investigate,

enforce, or assist in the investigation or enforcement of any federal criminal immigration law that penalizes a person's presence in, entry, or reentry to, or employment in, the U.S., as defined per Section 7284.4(f) GC. This restriction does not pertain to any information that is regarding a person's immigration or citizenship status pursuant to Title 8, U.S. Code Sections 1373 and 1644.

(7) Automated Archive System.

(a) Background. The DOJ maintains state summary criminal history information consisting of the master record of information on criminals compiled by the attorney general's office. That information includes names, aliases, dates of birth, physical descriptions, fingerprints, palm prints, sex offender registry, CDCR records, date(s) of arrest(s), charges, dispositions, and other pertinent data. The DOJ also maintains a secure, dedicated communication system, which makes the summary criminal history information available to all law enforcement agencies in the state via a uniform statewide communications network. Law enforcement agencies throughout the state collect fingerprint "cards" and maintain them in various levels of automation. Many law enforcement agencies submit this information to DOJ. The AAS is a web-based application that provides online access to DOJ criminal and applicant file folders, which include fingerprint images and NIST records for local law enforcement agencies, as well as DOJ staff.

(b) Database Information. The AAS is accessed from a PC's Web browser in a secure Intranet Web environment. The AAS images conform to NIST standards. The AAS utilizes the secure DOJ communication network and adheres to CLETS PPPs. Users of AAS must have DOJ network connectivity. Each county, city, and federal agency wishing access must submit an application and be approved for access by DOJ. Each individual person wishing to access AAS must meet the security requirements and be authorized by their commander, Division Chief, and Division AAS administrator. The AAS database provides access to fingerprint "cards" maintained by California's law enforcement agencies, as well as a connection to photographs and data maintained by DOJ. The AAS network and application are maintained by the DOJ AAS program.

(c) Access.

1 Fingerprint images are only accessible to Class I, II, and III law enforcement agency personnel as defined in Section 1.3.1 A, B, & C of the CLETS PPPs. A Class I law enforcement subscriber is defined as a governmental agency having statutory powers of arrest and whose primary functions are that of apprehension and detection.

Class I subscribers include, but are not limited to, sheriff's departments, city police departments, CHP, DOJ, and the FBI. The application for AAS access must be signed by the Commissioner and approved by DOJ before access will be granted. A new AAS User Agreement shall be updated at least every three years, when the head of the agency changes, or immediately upon request from the DOJ AAS coordinator.

2 Field Divisions and Area personnel requesting access must submit an e-mail to their respective Division ISU coordinator for initial approval. Requests will then be forwarded to FSS for final approval. Field Support Section maintains a current roster of all personnel authorized access. Accordingly, FSS shall be notified as soon as possible by the Division ISU coordinator of anyone whose access to the system is no longer authorized.

(d) Security. The AAS contains information derived from mandatory CORI law, including arrest and applicant fingerprint images, palm prints, sex offender registration documents, various firearm documentation, CDCR records, probation and parole information, and case disposition documents, and therefore falls under CORI rules and statutes. All transactions are programmatically logged and subject to audit by the respective participating agencies and DOJ. All participants, nonuniformed and uniformed personnel, must be fingerprinted and have a fingerprint check response on file prior to being granted access to AAS. It is required that each employee having access to AAS sign the CLETS Employee/Volunteer Statement Form prior to operating or having access to AAS. These forms do not need to be completed if already on file as a result of departmental training procedures. Additional requirements may be added at an agency's discretion. User IDs and passwords ensure access security. Each person wishing to access AAS must complete a New User Account and/or Administrator Account Form. These forms are available through the DOJ AAS section and are to be maintained by each CHP Division's AAS administrator. Each person will assign their own user ID (6-8 characters). User IDs will deactivate after 45 days of nonuse and a new User ID will need to be established. User IDs and passwords are case sensitive. A default password will be assigned by each CHP AAS Division administrator initially, but to ensure security, the password must be changed the first time the system is accessed. The password can be changed as often as desired by the user. The AAS terminals and information must remain secure from unauthorized access. Access to information through AAS is on a right-to-know and need-to-know basis. Authorized personnel shall not inquire into their own record or have someone inquire for them. Accessing and/or releasing AAS information

for non-law enforcement purposes is prohibited and is subject to administrative action and/or criminal prosecution.

(e) The California Values Act. Pursuant to GC Title 1, Division 7, Chapter 17.25 (commencing with Section 7284), federal, state, or local law enforcement agencies shall not use any noncriminal history information contained within this database for immigration enforcement purposes. "Immigration enforcement" includes any and all efforts to investigate, enforce, or assist in the investigation or enforcement of any federal civil immigration law, and also includes any and all efforts to investigate, enforce, or assist in the investigation or enforcement of any federal criminal immigration law that penalizes a person's presence in, entry, or reentry to, or employment in, the U.S., as defined per Section 7284.4(f) GC. This restriction does not pertain to any information that is regarding a person's immigration or citizenship status pursuant to Title 8, U.S. Code Sections 1373 and 1644.

(8) International Criminal Police Organization.

(a) Background. As the world's largest international police organization, INTERPOL's mission is to facilitate the exchange of police information and promote cooperation and assistance between law enforcement authorities. With its international presence, INTERPOL provides investigative resources to its 190 member countries and their law enforcement officials. These resources include a secure communications network and databases containing information supplied by its member countries on terrorists, crimes, missing persons, stolen and lost passports and travel documents, stolen vehicles, stolen art and artifacts, and other law enforcement information.

1 The Emergency Notification and Tactical Alert Center (ENTAC) serves as the statewide INTERPOL liaison to the U.S. DOJ, National Central Bureau, in Washington, D.C.

(b) Database Information. Maintaining various automated databases, INTERPOL can provide a wide range of information which can be used as an "International NCIC." The Department primarily uses INTERPOL's I-24/7 INSYST eAST2 database system which provides information on passport status (e.g., lost, stolen, or fraudulent), Stolen Vehicle System, and Employment Verification. In addition to the database access, ENTAC facilitates investigative assistance and information sharing with participating countries.

(c) Access. The INTERPOL databases are to be used for official use only as a criminal or background investigation resource. Inquiries into the

database or requests for investigative information from foreign jurisdictions are limited to personnel assigned to ENTAC.

1 Uniformed personnel who require information from INTERPOL or assistance from foreign jurisdictions may contact ENTAC by telephone or e-mail at Interpol@chp.ca.gov.

OFFICE OF THE COMMISSIONER ANNEX A

OPI: 065

THIS PAGE INTENTIONALLY LEFT BLANK

ANNEX A

TITLE 28, CODE OF FEDERAL REGULATIONS, PART 23

23.1 Purpose.
23.2 Background.
23.3 Applicability.
23.20 Operating principles.
23.30 Funding guidelines.
23.40 Monitoring and auditing of grants for the funding of intelligence systems.
Authority: 42 U.S.C. 3782(a); 42 U.S.C. 3789g(c).
§ 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 organization which is reasonably suspected

ANNEX A

TITLE 28, CODE OF FEDERAL REGULATIONS, PART 23 *(continued)*

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 manmade disaster;

ANNEX A

TITLE 28, CODE OF FEDERAL REGULATIONS, PART 23 *(continued)*

(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 ensure 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.
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) 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

ANNEX A

TITLE 28, CODE OF FEDERAL REGULATIONS, PART 23 *(continued)*

policy making authority who has been expressly delegated such control and supervision by the head of the agency:
(1) Assume official responsibility and accountability for actions take in the name of the joint entity, and
(2) 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 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. § 23.40 Monitoring and auditing of grants for the funding of intelligence systems.
(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.

THIS PAGE INTENTIONALLY LEFT BLANK