CALIFORNIA HIGHWAY PATROL

GENERAL ORDER 100.82

REVISED APRIL 2019

CHP 302A, FIELD INTERVIEW

1. PURPOSE. The purpose of this General Order (GO) is to establish policy and procedures for all field personnel regarding the use of the Department's CHP 302A, Field Interview (Annex A). This will include proper utilization, accurate completion, and retention of CHP 302As consistent with the guidelines established in Title 28, Code of Federal Regulations (CFR), Part 23 (28 CFR Part 23) (Annex B). All information entered on a CHP 302A is discoverable under the Public Records Act. All information entered must be professional in nature and in compliance with applicable laws and departmental policies.

2. POLICY.

a. Division commanders are responsible for ensuring proper use of the CHP 302A, in compliance with state and federal laws, as well as departmental policy. Divisions and Areas utilizing CHP 302As shall develop standard operating procedures (SOP) relative to their specific needs. These guidelines shall be in compliance with this GO; Division 3, Title 1.8, Chapter 1 of the California Civil Code (CCC); Title 1, Division 7, Chapter 3.5 of the California Government Code (GC); Highway Patrol Manual 11.1, Administrative Procedures Manual, Chapter 13, Information Disclosures - Public Records and Rights of Privacy; and 28 CFR Part 23.

b. The following shall apply:

(1) When utilizing the CHP 302A, officers shall record as much personal information as possible within the spaces provided. This pertains only to information that can be legally obtained (i.e., CCC Section 1798.14 states, "shall maintain in its records only personal or confidential information which is relevant and necessary").

Generally speaking, if there is something specific which might connect the person to a crime, completing a CHP 302A would be appropriate (Rodriguez – [1993] 21 Cal.App.4 232; 238-240, Harness [1983] 139 Cal.App.3d 226; and CCC Section 1798.14).

(2) All CHP 302As shall be maintained in a secure environment with access restricted to authorized personnel. Access to electronic databases should be given to those authorized by the commander who have both a legal right-to-know and the need-to-know.

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

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

This is to ensure the security and confidentiality of the information stored and to ensure the protection of the individual's right to privacy.

(3) All CHP 302As shall be stored and sorted by year, month, and day. This will facilitate any necessary future research of the form and ensure timely purging of the files according to 28 CFR Part 23.

(4) Field photographs are defined as a photograph taken of a person during a contact, detention, or arrest in the field. Booking photographs and undercover surveillance photographs of an individual are not considered "field photographs." Before photographing any field detainee, the officer shall carefully consider, among other things, the following factors:

(a) Field photographs may be taken when the subject of the photograph knowingly and voluntarily gives consent.

(b) Field photographs may be taken without consent only if the photograph is taken during a detention based upon reasonable suspicion of criminal activity. Knowledge or suspicion of gang membership or gang affiliation alone **is not** sufficient to justify a detention.

(c) Photographs taken during field interviews shall be attached to the CHP 302A. Photographs taken during an incident where a crime report was written shall be placed into evidence.

(5) No detention shall be prolonged for the sole purpose of taking a photograph.

(6) The information recorded on the CHP 302A, as well as an accurate accounting of the date, nature, and purpose of each disclosure of information, shall only be released on a right-to-know and need-to-know basis. The accounting of each disclosure shall also include the name, title, and business address of the person or agency to whom disclosure was made. **An accounting of disclosure of information between law enforcement**

officers actively engaged in duties in the field is not required (CCC, Section 1798.25). These disclosure accounts shall be retained for three years or until the record is destroyed (CCC, Section 1798.27).

(7) All information retained shall be maintained until the case is adjudicated (if applicable), is no longer relevant, or no pertinent "activity" has occurred within a five-year period necessitating an update to the information (28 CFR part 23). Once the information is deemed as no longer needed, it shall be destroyed.

(8) Area SOP concerning the CHP 302As shall be reviewed annually in order to ensure files are current, accurate, and relevant to departmental needs and objectives.

3. GENERAL.

a. The need to gather an individual's personal information for the purpose of tracking and establishing criminal trends, methods of operation, and organized criminal intent has long been recognized. Currently, CHP 302As are used by this law enforcement agency on a daily basis for documenting varying types of encounters with individuals. The information may be recorded and maintained for the purpose of identifying individual criminal offenders, alleged offenders, and for criminal investigations (including reports of informants).

b. As the Department's role has changed, so has the need for gathering criminal intelligence for individuals suspected of illegal activity. Therefore, it has become increasingly necessary to maintain intelligence files of possible suspects, suspected criminal activity, and methods of criminal operations by utilizing CHP 302As and/or entering information into electronic databases.

4. CRIMINAL INTELLIGENCE FILES.

a. The purpose for criminal intelligence files is to provide a law enforcement agency with an information base which meets the needs of the agency in carrying out its efforts to protect the public and suppress criminal operations.

b. A criminal intelligence file may contain information related to the following:

(1) Individuals who:

(a) Are suspected of being or have been involved in the actual or attempted planning, organizing, financing, or commission of criminal acts.

(b) Are suspected of being or have been involved in criminal activities with known or suspected crime figures.

(2) Organizations, businesses, and groups which:

(a) Are suspected of being or have been involved in the actual or attempted planning, organizing, financing, or commission of criminal acts.

(b) Are suspected of being or have been illegally operated, controlled, financed, or infiltrated by known or suspected crime figures.

c. Criminal intelligence files are not public record and are exempt from public disclosure pursuant to GC Section 6254(f). Generally, the information is disseminated on a right-to-know or need-to-know basis.

5. RETENTION.

a. All information retained in a criminal intelligence file shall be maintained as such until the case is adjudicated (if applicable), is no longer relevant, or no pertinent "activity" has occurred within a five-year period necessitating an update to the information (28 CFR Part 23). Once the information is deemed as no longer needed, it shall be destroyed.

b. There are two categories relating to the retention of gathered information:

(1) Permanent Status.

(a) Information which relates that an individual, organization, business, or group is suspected of being or has been involved in the actual or attempted planning, organizing, financing, or committing of criminal activity.

(b) A list of crimes which would warrant the gathering of information on a group or individual. This includes, but is not limited to, the following:

1 Extortion.

2 Narcotics/drug trafficking.

3 Loan sharking.

4 Bribery.

5 Major crimes including homicides, sexual assaults, burglary, auto theft, kidnapping, destruction of property, robbery, fraud, fencing of stolen property, and arson.

6 Manufacture, use, or possession of explosive or destructive devices for the purposes of fraud, intimidation, or political motivation.

7 Threats to public officials and private persons including terrorist threats.

8 Any person who promotes, furthers, or assists any criminal street gang.

(c) In addition to falling within the confines of one or more of the above crimes, the suspect/entity to be given permanent status in an intelligence file must be identifiable. This can be by name or unique identifying characteristics (e.g., date of birth, criminal identification number, driver license number, or home/business address). Identification at the time the file is created is necessary to distinguish the subject/entity from existing file entries and those that may be entered at a later date.

NOTE: The exception to this rule involves modus operandi files. Modus operandi files describe a unique method of operation for a specific type of crime and may not be immediately linked to an identifiable suspect. Modus operandi files may be retained indefinitely while additional identifiers are sought.

(2) Temporary Status.

(a) Information which does not meet the criteria for permanent storage but may be pertinent to an investigation involving one of the categories previously listed should be given temporary status. It is recommended that retention of “temporary” information not exceed a five-year period unless a compelling reason exists. (An example of a compelling reason would be a situation in which someone has several pieces of information indicating that a crime has been committed, but is unable to identify the suspect within five years, and it is believed that with additional time, a proper identification can be made.) During this time period, efforts should be made to identify the subject/entity or validate the information so that the final status may be determined. If the information is still classified “temporary” at the end of the five-year period and a **compelling** reason to retain the information is not evident, the information **should** be purged.

(b) An individual, organization, business, or group may be given temporary status in the following cases:

1 Subject/Entity is Unidentifiable. Subject/entity is suspected of being engaged in criminal activity and has no known physical descriptors, identification numbers, or distinguishing characteristics available.

2 Involvement is Questionable. Involvement by a subject/entity in criminal activity is suspected. This involvement has either:

a Possible Criminal Associations. An individual, organization, business, or group (not currently reported to be criminally active) associates with a known criminal and appears to be jointly involved in illegal activities.

b Criminal History. An individual, organization, or group (not currently reported to be criminally active) has a history of criminal conduct, and the circumstances currently being reported (e.g., new position or ownership in a business) indicate they may again become criminally active.

b. Area SOP concerning intelligence files shall be reviewed annually in order to ensure the file is current, accurate, and relevant to the needs and objectives of the Department.

6. RELEASE OF INFORMATION. The separation of public information from criminal intelligence files can better protect the confidentiality of the criminal file. If a request is made for public records (e.g., subpoena, court order), an agency can release the public file and leave the intelligence file intact.

OFFICE OF THE COMMISSIONER ANNEXES A, B

OPI: 065

ANNEX A

CHP 302A, FIELD INTERVIEW

NAME	AKA / MONIKER	DL NUMBER	DATE	TIME
DOE JOHN	SLEEPY	B0000000	3/10/03	1015

RESIDENCE ADDRESS/CITY/STATE	HOME PHONE
1015 3RD STREET SACRAMENTO CA	(916) 555-0000

OCCUPATION/STUDENT	BUSINESS/SCHOOL	CELL PHONE
UNEMPLOYED	N/A	(916) 555-1000

DOB	RACE	SEX	HEIGHT	WEIGHT	HAIR	EYES
10/15/1976	WHITE	M	6-01	200	BRN	BRN

FACIAL HAIR	HAIR DESCR.	GLASSES (Circle)	PARENT NAME	CONTACTED (Circle)
NONE		YES / (NO)	N/A	YES / (NO)

SCARS / MARKS / TATTOOS / BODY PIERCINGS
TATTOO - GRN CLOVER (LEFT ARM)

HAT	JACKET	TOP	BOTTOM	SHOES
N/A	BLACK	WHITE T-SHIRT	BLACK PANTS	BLACK BOOTS

VEH YEAR	MAKE	MODEL	STYLE	COLOR	LICENSE / STATE	OTHER
1989	BMW	325i	2-DOOR	BLK	1ABC234	

CALL SIGN	BEAT	LOCATION
123-4	4	N/B I-5 AT RICHARDS BLVD.

PROBATION (Circle)	P.O. NAME	SEARCH TERMS	OFFICER'S NAME / ID#
(PAROLE)	MR. SMITH	PAROLE	STRAHAN # 12345

FIELD INTERVIEW, CHP 302A (Rev. 11-06) OPI 065

FRONT SIDE

REASON FOR F.I. *(Circle one)*

(TRAFFIC)	PEDESTRIAN	DRUG RELATED	REPT. PARTY	(INTOX/UI)	FIRE	OFF ROAD	TRESPASS
WITNESS	POSS. SUSPECT	GANG RELATED	ILL. PARKED	BICYCLE	5150	DOMESTIC VIOLENCE	
VICTIM	SUSP. VEHICLE	SUSP. SUBJECT	VANDALISM	OTHER:			

GANG MEMBER ADMISSION *(Circle one)*
(YES) NO GANG NAME: ARYAN BROTHERHOOD
EXACT STATEMENT: "I'M IN THE A.B."

GANG INFORMATION *(Circle criteria if applicable & describe below)*

(ADMISSIONS)	(GANG TATTOOS)	GANG ARREST	GANG GRAFFITI	GANG DRUG SALES	GANG M.O.	
OTHER AGENCY	GANG WRITINGS	FAMILY INFO.	(GANG ATTIRE)	INFORMANT INFO.		
OBS'D W/ GANG MEMBER		ASSOC. W/ GANG ACTS				

NAME	DOB	NAME	DOB
DOE BOB	7/23/81	DOE JOE	9/20/1975

2nd VEH YEAR	MAKE	MODEL	STYLE	COLOR	LICENSE / STATE	OTHER
1990	HONDA	CIVIC	2-DOOR	BLK	2ABC345	

ADDITIONAL INFORMATION
ALL SUBJECTS CONTACTED WERE ON PAROLE.

FIELD INTERVIEW, CHP 302A (Rev. 11-06) OPI 065 (Reverse)

BACK SIDE

THIS PAGE INTENTIONALLY LEFT BLANK

ANNEX B

TITLE 28, CODE OF FEDERAL REGULATION, PART 23

PART 23-CRIMINAL INTELLIGENCE SYSTEMS OPERATING POLICIES.
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 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 manmade 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) 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:
(1) assume official responsibility and accountability for actions taken 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 participating agencies will be in compliance with the principles set forth in § 23.20. 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 CFR23 Criminal Intelligence Systems Policies.

THIS PAGE INTENTIONALLY LEFT BLANK