

**CALIFORNIA LAW ENFORCEMENT
TELECOMMUNICATIONS SYSTEM (CLETS)**

**FULL ACCESS OPERATOR
WORKBOOK**

July 2011



Prepared by:

**California Department of Justice
Client Services Program**

**KAMALA D. HARRIS
ATTORNEY GENERAL**

INTRODUCTION

INSTRUCTIONS FOR AGENCY CLETS COORDINATORS, TRAINING OFFICERS AND/OR SUPERVISORS

The California Law Enforcement Telecommunications System (CLETS) Policies, Practices and Procedures (PPPs) (Section 1.8 – Training) and the National Crime Information Center (NCIC) Operating Manual (Section 3 – Quality Control, Validation, and Other Procedures) state the following regarding CLETS/NCIC training:

Initially (within six months of employment or assignment) train, functionally test, and affirm the proficiency of terminal (equipment) operators (FULL ACCESS/LESS THAN FULL ACCESS) in order to ensure compliance with CLETS/NCIC policies and regulations.

A Full Access (Update) Operator is defined as an operator who has a CLETS User ID and password and makes inquiries into the systems and/or performs update functions. A Less Than Full Access (Inquiry) Operator has a CLETS User ID and password and only makes inquiries into the systems.

This telecommunications workbook is designed to meet the aforementioned requirements and combines BOTH the FULL ACCESS and the LESS THAN FULL ACCESS workbooks into one document. Each section of the workbook is clearly marked, i.e., Section One Combined and Section Two Full Access. **The Full Access operator MUST complete Sections One and Two.**

- A. As the operator completes a chapter of the workbook, review that chapter and record the completed date on the appropriate Completion Log in that section. Because some individuals access selected databases only, ALL operators must complete the chapters on General Policies and Liability/Security Issues, CLETS, Criminal Justice Information System (CJIS), and then those chapters of the workbook related to their job assignment. In Section Two, Full Access operators must complete the chapters on Record Maintenance and CLETS, and then those chapters of the workbook related to their job assignments.
- B. The completed workbook should be kept by the operator as reference material. Training records must be maintained, reflecting the level of the operator (Full Access or Less Than Full Access), the date the operator completed CLETS training and the date the operator completed the workbook. If the agency maintains a score for the workbook, 70% is considered passing.
- C. Workbooks need only be completed once in an operator's career. However, recertification is required biennially for both Full Access and Less Than Full Access terminal operators. This is accomplished by completing the current CLETS Operator Proficiency Examination, as provided by the Department of Justice (DOJ) Client Services Program, and obtaining a score of at least 70%. Training records must indicate the date the recertification exam was completed and either the final score or a pass notation. Training records will be periodically audited by the NCIC and the DOJ.

This proficiency examination is available for downloading by accessing the DOJ California Law Enforcement Web (CLEW) site at <http://clew.doj.ca.gov>. Select Field Operations, Downloads/Publications. It is also available as an online examination at the Client Services Program (Field Operations) link. The website address is: <http://fieldops.doj.ca.gov/fieldops.asp>. The User ID is "fieldops" and Password is "D0j1066! (Capital D, Zero, lower case j, 1066 exclamation point). The User ID and password are case sensitive and are the same for all users. The on-line exams require that all questions be answered before submitting. If you have any questions, please contact the DOJ Client Services Program at (916) 227-3332.

EMPLOYEE/VOLUNTEER STATEMENT FORM

**USE OF CLETS CRIMINAL JUSTICE INFORMATION
AND DEPARTMENT OF MOTOR VEHICLES RECORD INFORMATION**

As an employee/volunteer of _____, you may have access to confidential criminal records, Department of Motor Vehicle records, or other criminal justice information, much of which is controlled by statute. All access to California Law Enforcement Telecommunications System (CLETS) related information is based on the need-to-know and the right-to-know. Misuse of such information may adversely affect an individual(s) civil rights, and violates the law and/or CLETS policy.

Penal Code section 502 prescribes the penalties relating to computer crimes. Penal Code sections 11105 and 13300 identify who has access to criminal history information and under what circumstances it may be released. Penal Code sections 11141-11143 and 13302-13304 prescribe penalties for misuse of public record and CLETS information. California Vehicle Code section 1808.45 prescribes the penalties relating to misuse of Department of Motor Vehicle record information. Penal Code sections 11142 and 13303 states:

Any person authorized by law to receive a record or information obtained from a record who knowingly furnishes the record or information to a person not authorized by law to receive the record or information is guilty of a misdemeanor.

Any person/volunteer who is responsible for CLETS misuse is subject to immediate dismissal from employment. Violations of the law may result in criminal and/or civil action.

I HAVE READ THE ABOVE AND UNDERSTAND THE POLICY REGARDING MISUSE OF ALL CLETS ACCESSIBLE INFORMATION.

Signature: _____

Print Name: _____

Date: _____

**SECTION ONE
FULL ACCESS AND LESS THAN FULL ACCESS OPERATOR
COMBINED WORKBOOK
COMPLETION LOG**

Employee Name: _____

The Agency CLETS Coordinator (ACC) or supervisor administering the training must date and initial each completed chapter. All operators must complete Chapters A, B and C, and then only those databases pertinent to their job assignments. Employees should maintain a copy of this log for their records.

CHAPTER	COMPLETION DATE	INITIALS
A. <u>General Policies and Liability/Security Issue</u>	_____	_____
B. <u>California Law Enforcement Telecommunications System (CLETS)</u>	_____	_____
C. <u>Criminal Justice Information System (CJIS)</u>	_____	_____
D. <u>Criminal History System (CHS)</u>	_____	_____
E. <u>Wanted Persons System (WPS)</u>	_____	_____
F. <u>California Restraining and Protective Order System (CARPOS)</u>	_____	_____
G. <u>Supervised Release File (SRF)</u>	_____	_____
H. <u>Missing and Unidentified Persons System (MUPS)</u>	_____	_____
I. <u>Sex and Arson Registration (SAR) - Violent Crime Information Network (VCIN)</u>	_____	_____
J. <u>Stolen Vehicle System (SVS)</u>	_____	_____
K. <u>Automated Boat System (ABS)</u>	_____	_____
L. <u>Automated Property System (APS)</u>	_____	_____
M. <u>Automated Firearms System (AFS)</u>	_____	_____
N. <u>Mental Health Firearms Prohibition System (MHFPS)</u>	_____	_____
O. <u>Armed Prohibited Persons System (APPS)</u>	_____	_____
P. <u>Automated Archive System (AAS)</u>	_____	_____
Q. <u>Department of Motor Vehicles (DMV)</u>	_____	_____
R. <u>National Crime Information Center (NCIC)</u>	_____	_____
S. <u>National Law Enforcement Telecommunications System (NLETS)</u>	_____	_____
T. <u>Oregon Law Enforcement Data System (LEDS)</u>	_____	_____

SECTION ONE
FULL ACCESS AND LESS THAN FULL ACCESS OPERATOR
COMBINED WORKBOOK

A. GENERAL POLICIES AND LIABILITY/SECURITY ISSUES

To ensure the security and integrity of the CLETS/NCIC systems, the California Code of Regulations states that a record check (fingerprint) shall be conducted on all personnel who have access to CLETS provided information. Personnel shall not operate or have access to CLETS terminals, equipment or information until a background and fingerprint check is completed and approved by the agency head, and an “Employee/Volunteer Statement Form” has been signed. The CLETS “Policies, Practices, & Procedures” (PPPs) states that if a fingerprint check reveals a felony conviction of any kind, CLETS access shall **NOT** be granted. In addition, all CLETS equipment must be secure from access by unauthorized personnel. Access to, or transmission of, CLETS information through the Internet is permitted when all requirements stated in the PPPs Section 1.9.4 are met. **All CLETS provided information (including DMV) is confidential and for OFFICIAL USE ONLY.** Access to CLETS information is only allowed upon a “right to know” and “need to know” justification. Authorized personnel shall not inquire into their own record or have someone inquire for them. The DOJ has established test message keys and test records that should be used for training or testing purposes. Do not use live criminal records when conducting training sessions. See DOJ Information Bulletin 97-12-BCIA for a list of the test records. Accessing and/or releasing CLETS information for non-law enforcement purposes is prohibited, unless otherwise mandated, and is subject to administrative action and/or criminal prosecution. All CLETS users must be assigned a unique User ID and password in order to access CLETS. Sharing your User ID and password is prohibited.

B. CALIFORNIA LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEM (CLETS)

The CLETS network is a high-speed message switching system located in Sacramento with a backup system in Orange County. This network provides law enforcement and criminal justice agencies access to the DOJ Criminal Justice Information System, Federal Bureau of Investigation (FBI) NCIC, National Law Enforcement Telecommunications System, Oregon Law Enforcement Data System, and California Department of Motor Vehicles.

It is critically important for all CLETS operators to adhere to the following: A computer match on a person or property is not probable cause for arrest or confiscation in and of itself. Confirmation with the originating agency to determine if the person or property is still wanted and is probably the same as the person or property of inquiry is **required**. Because names, physical descriptions, and property descriptions are not unique, **DO NOT TAKE ANY FURTHER POLICE ACTION BASED ON A “HIT” UNTIL IT IS CONFIRMED THAT THE PERSON OR PROPERTY IS THE SAME AS THAT OF AN ACTIVE RECORD.** The agency confirming the hit must access the originating agency’s “Master Case Record” for current status and information. The Master Case Record must be available at all times for confirmation.

All transactions require the submission of an agency’s ORI (ORIGINating agency identifier), assigned by the NCIC to identify each agency. The ORI is a nine-character agency identifier. Using CA0349454 as an example from the DOJ Missing and Unidentified Persons Unit (MUPS) in Sacramento, the ORI is formatted as follows: CA = state code; 034 = county code, in alphabetical sequence; 94 = agency identifier (00 is always a sheriff’s department, 94 is DOJ, 99 is always a California Highway Patrol office); and 54 = a sub-station or unit within an agency (MUPS), or a

criminal justice agency. More information is available on ORIs from the NCIC 2000 Operating Manual, ORI File, ORI Structure.

In addition to accessing law enforcement records regarding persons or property, CLETS provides users with the ability to transmit point-to-point free-text Administrative Messages (AM) to other agencies within California using agency mnemonics and/or group codes, and to out-of-state agencies using ORIs. AMs can be sent to a combination of up to six addresses at one time. All Points Bulletins (APB) are free text messages sent to all LEAs in California, or directed to participating agencies in specific groups by using Group Codes and sub group codes (e.g., highway, geographic, crime specific, all sheriffs, all police, and all counties). An example of a crime specific group is the Child Abduction Alert group code 4500, which is a statewide broadcast to all law enforcement agencies regarding child abduction. An APB can also include major identifiable property crimes, crimes against persons, Be-On-The-Look-Out (BOLO) notices, officer death and funeral notices, law enforcement training, seminar and meeting announcements, and acts of nature. Refer to the CLETS Operating Manual, and the NLETS section in this document for further information.

C. CRIMINAL JUSTICE INFORMATION SYSTEM (CJIS)

The CJIS data systems are maintained by the California DOJ and are available to authorized local, state and federal criminal justice agencies, pursuant to California Government Codes 15150-15167, via the CLETS network. To ensure your agency has the most current information for accessing and updating the systems, refer to the California Law Enforcement Web-site (CLEW) at <http://clew.doj.ca.gov> for all operating manuals and DOJ Information Bulletins.

The California CJIS data systems available through CLETS are:

Criminal History System (CHS)	Stolen Vehicle System (SVS)
Wanted Persons System (WPS)	Automated Boat System (ABS)
Supervised Release File (SRF)	Automated Property System (APS)
Missing and Unidentified Persons System (MUPS)	Automated Firearms System (AFS)
Sex and Arson Registration (SAR)–	Mental Health Firearms Prohibition
Violent Crime Information Network (VCIN)	System (MHFPS)
Armed Prohibited Persons System (APPS)	California Restraining & Protective Order
	System (CARPOS)

Penal Code (PC) section 11108 requires “each sheriff or police chief executive shall submit descriptions of serialized property, or non-serialized property that has been uniquely inscribed, which has been reported stolen, lost, found, recovered, held for safekeeping, or under observation, directly into the appropriate CJIS automated property system for firearms, stolen bicycles, stolen vehicles, or other property, as the case may be.” When a California law enforcement agency enters a record into any of the CJIS data systems, a unique File Control Number (FCN) is generated for each successful entry. The FCN is a thirteen-digit number generated by the CJIS. Using 1860203500123 as an example, the FCN is formatted as follows: 186 = agency identifier; 02 = year of entry; 035 = day of year; 00123 = daily transaction number. Each CJIS database can have 99,999 records entered daily. In most systems, the FCN will retrieve the most complete and comprehensive record available, as opposed to an abbreviated or summary record in response to a name inquiry. It is also used to authenticate an agency in order for them to modify or cancel their record.

Within the CJIS, a name inquiry will cause the last name to be searched by the sound-a-like system (Soundex), and the first name will be searched using the diminutive tables. With the Soundex system, an inquiry on John Schultz may match a record with the last name of Shuels. Carefully read your

responses. With the diminutive tables, a name inquiry on Greg will also search records with the name Gregg and Gregory. Creative spelling of names, such as Karyn, Chayse, etc. will not provide matches. When inquiring on unique or ethnic names, it may be helpful to use the initial of the first name, along with the last name, gender and date of birth. The use of sex code X (Unknown) is recommended for name inquiries as the search will be run against male, female and unknown records. An exception is the Missing Persons System, which requires an inquiry with either male or female only.

Using the subject's date of birth is recommended as the inquiry will be forwarded to NCIC for a search of their person files. In the CJIS Criminal History System, a date of birth inquiry will search that date plus or minus three years, for a six year range. For age, the search is that year plus or minus three years for a seven year range. In the other CJIS person files, a date of birth inquiry will search that date plus or minus one year for a two year range, or if age is used the inquiry will search that year plus or minus three years for a seven year range. Keeping this information in mind is useful when an individual has used many dates of birth. There may be a warrant that isn't retrieved, because that particular record was entered with a date of birth outside your search range. These name search recommendations work with the CJIS databases, but not with DMV or necessarily other state or national systems.

D. CRIMINAL HISTORY SYSTEM (CHS)

The CHS is the central repository for Criminal Offender Record Information (CORI) and applicant record information. CORI is defined in Penal Code (PC) section 11075 as a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges, sentencing, incarceration, rehabilitation and release. In order to access CORI, the "right-to-know" and "need-to-know" (also known as compelling need) must be established. The right-to-know means the right to obtain CORI pursuant to court order, statute, or decision law. The need-to-know means the necessity to obtain CORI in order to execute official responsibilities. Examples of compelling needs include when a subject is in custody or may be a suspect in a criminal investigation. A preliminary record check may be performed on any person prior to their approval as a "ride-along" with a law enforcement officer (or "sit-along" with a dispatcher), provided the person is not an employee of the law enforcement agency. Also, the fingerprint background process must not be circumvented by running applicants through the Criminal History System prior to a "ride-along" or "sit-along". For facility security purposes, staff of a correctional/detention facility may process on-line criminal history inquiries on any visitor. Again, the results of that inquiry should not be shared with any hiring authority. Remember, even though you may be authorized to receive CORI by statute, there must be an official business need before any requests for CORI are initiated.

Use of CORI for other than official business need may be a violation of PC sections 502, 11105, 11140-11143, and 13301-13304. PC section 11142 states, "any person authorized by law to receive a record or information obtained from a record who knowingly furnishes the record or information to a person who is not authorized by law to receive the record or information is guilty of a misdemeanor." There have been sworn and non-sworn law enforcement/criminal justice personnel who have been terminated and prosecuted for using CORI for other than official business.

In addition to the restrictions mentioned above, law enforcement agencies are not authorized to access CORI through CLETS for licensing, employment, certification purposes, or for a record review and/or challenge by the subject of a record. Applicant fingerprints, via Livescan, must be submitted for these purposes. Agencies authorized access to the Criminal History System must maintain an audit trail whenever CORI is furnished to another agency. The audit trail must be available for inspection for not less than three years [707(c) California Code of Regulations (CCR)]. In addition, fingerprint

background checks shall be conducted on all personnel hired after July 1, 1975 who have physical access to the computer system, its terminals or the stored CORI [707(b) CCR].

Additionally: The very use of CLETS for other than official law enforcement purposes may result in your dismissal and/or possible prosecution.

The CHS is comprised of the Master Name Index (MNI), the Automated Criminal History System (ACHS) and the Manual Criminal History System. The MNI is predominately used when only the subject's name and/or personal identification number (Date of Birth, Social Security Number, California Driver's License Number, FBI Number, or Institution Number) is available. Refer to the CJIS section for more information on conducting searches with name, sex and date of birth.

Within the CHS there are various types of criminal history records, commonly called "rap sheets," three of which are available on-line:

- Automated:* The letter "A" precedes the state identification number (CII) to identify it as a fully automated record.
- Hybrid:* The letter "H" precedes the CII number and identifies a manual record that has been partially automated. The response on a Hybrid record will display a flag identifying it as such. The automated portion is available on-line and the manual portion is available by contacting the DOJ Command Center. It is important to request the manual portion in order to get the entire record.
- Disposition:* Also known as a DSP record is identified as a nine character (all numeric) number and is accessible by using the same inquiry format(s) used for an automated CII record. A DSP is not based on fingerprint identification, and will contain a warning that states: "This record is based upon an arrest or court disposition report. The lack of fingerprints prevents positive identification. Use of this information is the receiver's responsibility."
- Manual:* The letter "M" precedes the CII number and identifies a record that is a manual file not automated in the Criminal History System, and must be requested from the DOJ Command Center via phone, fax, teletype, mail or in person. Their phone number is 916-227-3244.

A mandatory route field (RTE) must be completed for all ACHS inquiries, via CLETS. This 30 character field must indicate the name, initials or ID# of the CLETS operator, the person requesting the record, if different, and the specific reason for the request, such as a case #, arrest #, booking #, warrant #, code violation #, etc. Among others, "investigation" and "narcotic investigation" are not acceptable reasons.

The DOJ Command Center no longer provides name based criminal history checks for peace officer pre-employment screening. Advancements in electronic fingerprinting have rendered this service obsolete. As a reminder, CLETS shall not be used by agencies to conduct CORI pre-employment background checks for peace officer applicants.

CORI may be faxed from one secure location to another secure location. When printed CORI is no longer needed, Title II, section 708(a) of the CCR requires the destruction of CORI in such a manner that the identity of the subject can no longer be ascertained. CORI stored on electronic media must be destroyed in the same manner.

E. WANTED PERSONS SYSTEM (WPS)

The WPS is a pointer system that pertains to arrest warrants maintained by state, local, and federal criminal justice agencies. When an inquiry results in a positive match, or hit, and it appears the person is the same as the person of inquiry, the inquiring agency must teletype the originating agency of the record for confirmation purposes, using the NLETS YQ message. NCIC policy requires YQ/YR transactions be used for all hit confirmation requests and responses. In addition to the YQ/YR transaction, agencies can confirm or request confirmation via telephone provided the phone conversation is recorded in some manner in the event the record is later not confirmed as valid by the entering agency.

A match made on a WPS record does not, by itself, provide sufficient grounds to arrest a person. You must confirm the descriptors are the same and the warrant is still outstanding. The originating agency must provide a 'substantive' response, using a YR teletype message, indicating the subject is the same as that of the inquiry (hit confirmed), is not the same as (hit denied) or an approximate time when they will be able to confirm or deny the hit. A response to an urgent request should be provided within ten minutes, and a response to a routine request should be provided within one hour.

All WPS records must be based on an arrest warrant. The warrant/Master Case Record must be maintained by the wanting agency and available at all times for confirmation. An agency may enter a wanted person into the WPS whether the agency is willing or unwilling to transport that person from anywhere in California. The Entry Level (ENT) indicates the agency's intent. ENT/1 (CA only) or 2 (CA & NCIC) – agency is willing to transport, ENT/3 or 4 - agency unwilling to transport (CA only). All ENT/1 felony warrants that contain NCIC required fields will programmatically be sent by the WPS to NCIC and the ENT/ will be changed to 2 when the NCIC returns the NIC number. The record will be forwarded to NCIC with the notation 'NOEX OUTSIDE CA' in the beginning of the miscellaneous (MIS) field, indicating the entering agency is not willing to extradite the wanted person from outside California.

Inquiries into the WPS may be made with the subject's name and sex. CLETS will forward the inquiry to NCIC only if a date of birth or other numeric identifier is included with the name and sex. Refer to the CJIS Manual, section 3.12 for more information on conducting searches with name, sex and other optional data fields.

F. CALIFORNIA RESTRAINING AND PROTECTIVE ORDER SYSTEM (CARPOS)

The Domestic Violence Restraining Order System (DVROS) has been renamed the California Restraining and Protective Order System (CARPOS). The CARPOS is a pointer system that contains restraining and/or protective order information on individuals who are the subject of a court order and entered by California law enforcement agencies. Information in the CARPOS is used by law enforcement to identify persons named in restraining and/or protective orders and to receive the terms and conditions of the orders. All records entered into the CARPOS must be based on a Master Case Record maintained by the entering agency. The CARPOS data base contains several types of restraining/protective orders including, but not limited to: Emergency Protective Orders, Juvenile Orders, Temporary & Permanent Workplace Harassment Orders, Criminal Protective Orders, Temporary & Permanent Civil Harassment Orders, Temporary & Permanent Elder and Dependent Adult Abuse Orders, Out-of-State orders, and Domestic Violence Restraining Orders. Mandated orders must be entered into the CARPOS, whether served or unserved. Entries that meet NCIC criteria are automatically forwarded to NCIC's Protection Order File. Out-of-State orders must be registered with a California court to be entered in the CARPOS.

An inquiry can be made into the CARPOS by using the file control number (FCN), agency case number (OCA), or name and sex of the restrained person(s) or protected person(s). A name inquiry into the WPS or the Supervised Release File (SRF) automatically searches the CARPOS. Refer to the CJIS Manual section 6.14 for more information on conducting searches with name, sex and date of birth.

Various California Code Sections contain provisions that prohibit persons subject to specific types of restraining/protective orders from owning, possessing, purchasing, or receiving any firearm while the order is in effect. The CARPOS allows reported violations of restraining/protective orders to be added to an existing order by any authorized agency as well as agencies with inquiry only capabilities. By entering a violation message, an agency establishes a statewide history of violations that are accessible to any law enforcement or criminal justice agency who may be conducting an investigation, building a stalking case, pursuing possible prosecution, or seeking a sentence enhancement on the subject of the restraining order. Records will remain in the history file for five years after the date of expiration or cancellation.

G. SUPERVISED RELEASE FILE (SRF)

The SRF is designed to provide law enforcement with an index of subjects on supervision or monitoring within California including: subjects on active parole from the California Department of Corrections and Rehabilitation and Division of Juvenile Justice, probationers entered by county and federal departments, sex and arson registrants updated from the Violent Crime Information Network, career criminals as defined by PC section 13853 and entered by law enforcement, and persons released under the supervision of the Department of Mental Health (DMH). Since June 2005, supervising parole and probation departments have had the ability to enter their records in both the California SRF and the NCIC SRF, making these records available nationwide. Since July 2008, the DMH has also had the ability to enter their records in both the California SRF and the NCIC SRF. When a record is designated as Entry Level 2, the SRF will automatically generate and submit an entry transaction for the NCIC SRF.

An inquiry through CLETS using the appropriate message key with name and sex will automatically search the SRF, the WPS and the CARPOS. Using a numeric identifier, such as date of birth, ensures a search of NCIC since the query is forwarded to the WPS. Refer to the CJIS section, (Chapter C) for more information on conducting searches with name, sex and date of birth. The SRF inquiry has been enhanced to include an option to search the new Armed Prohibited Persons System (APPS) along with SRF if desired. Refer to the APPS section for more information.

The SRF provides for a two-way communication link which allows law enforcement officers to send information about an encounter with a subject on supervised release to the agency that entered the record. This link is called a "Contact Message." After receiving information from the SRF about your individual, you are requested to send a Contact Message via CLETS to the agency that entered the record. The Contact Message summarizes your encounter with the subject, has a free text field for comments, such as, date, time and location of the encounter, and allows for the inclusion of any vehicle information. The Contact Message should be sent, whether encountered or not, if the person is a suspect in an investigation, if your agency is issuing a warrant, if they are being booked or cited, or even during a routine stop or field interview where no enforcement action is being taken. The Contact Message is transmitted through CLETS, matched to the SRF record, and forwarded to the agency which entered the record. The transmittal of the Contact Message to the originator of the SRF record is essential. Officers on the street can learn the status of the individuals they are encountering, while supervising agents and agencies interested in the activities of an individual can receive information on the nature of the contact. Parole agents have received Contact Messages indicating

possible criminal activity at a time when the subject was being considered for early release. Sending Contact Messages not only supports the efforts of the agencies supervising individuals in the SRF, it benefits all California law enforcement by tracking and monitoring these individuals and sharing this information statewide. The Contact Message is also a good way to formally document contact with a sex registrant, and indicate if any public notification took place in accordance with Megan's Law. If the SRF record is entered with the subject's CII number, the supervising agency automatically receives a Notice of Arrest from the DOJ after a new arrest has been updated to the subject's criminal history record.

The SRF has a full set of test/training message keys to eliminate the use of the production database (live records) for testing and training activities by agencies. The test message keys will support both ENT/1 (California SRF only) and ENT/2 (California SRF and NCIC SRF). Records entered or modified as ENT/2 will be passed to the test/training sides of NCIC SRF.

H. MISSING AND UNIDENTIFIED PERSONS SYSTEM (MUPS)

The MPS is a database of all persons, juvenile and adult, entered as missing by law-enforcement. PC section 14205(a) states in part that: "All local police and sheriffs' departments shall accept any report, including any telephonic report, of a missing person, including runaways, without delay and shall give priority to the handling of these reports over the handling of reports relating to crimes involving property." A missing person record is categorized as a: Stranger Abduction; Parental/Family Abduction; Runaway; Suspicious Circumstances; Catastrophe; Lost; Unknown Circumstances; Dependent Adult; or Missing Adult. All missing person entries are programmatically forwarded to NCIC. The MPS may be inquired on directly or as the result of a Wanted Person System search being returned from NCIC. The missing person record may also contain suspect and vehicle information. A record entered with the required vehicle data elements as a supplemental transaction will be forwarded to the Stolen Vehicle System (SVS) where a Missing Person Vehicle record is created and available when law enforcement inquires into the SVS with a vehicle license plate. In the event of a child abduction, an All Points Bulletin (APB) may be sent as an Administrative Message to group code 4500. This APB will be broadcast statewide. This broadcast should be initiated whether or not the abduction meets the criteria for an Amber Alert.

Photographs and dental/skeletal X-rays of missing persons should be sent to the DOJ MUPS Unit on all open cases. DNA samples may also be submitted. The DOJ MUPS Unit distributes posters and quarterly bulletins of missing persons to thousands of locations throughout California and the nation. All photographs of missing persons, juvenile or adult, received in the MUPS Unit are also placed on the California Attorney General's Internet website at <http://www.ag.ca.gov/missing>.

The Unidentified Persons System (UPS) is a database of unidentified persons, both living and deceased, and body parts from California and surrounding states. The UPS may include fingerprints and dental charts. A physical descriptor inquiry is accomplished in CJIS using physical characteristics of age, sex, race, and height. If weight, hair, and eye color are added, the inquiry is forwarded to NCIC. The two systems, MPS and UPS, are cross searched daily by NCIC for possible matches, and any possible hits (\$.M) are forwarded to the originating agency of each record to analyze.

I. SEX AND ARSON REGISTRATION (SAR) – VIOLENT CRIME INFORMATION NETWORK (VCIN)

California law mandates that persons convicted of specified sex and arson offenses have a lifetime requirement to register with their local police or sheriff's department. Juvenile arson offenders must

register for ten years following adjudication. Local law enforcement agencies who register offenders can enter and update sex and arson registration information directly into VCIN via the CLETS. A summary record of all sex and arson registrant records are updated into the SRF twice daily. The SRF sex and arson registrant records are considered tactical responses, whereas the VCIN registrant record is better suited for investigators because it contains additional data. VCIN contains a full comprehensive record including all physical descriptors, predator designations, registration history with addresses, vehicle information, etc. and is available by inquiring directly into VCIN with the subject's CII or FCN. Inquiry responses may also include notices of the subject's registration status, such as, "whereabouts unknown," "may not be in compliance..." etc. Refer to PC 290 for current sex registrant requirements and to PC 457.1 for current arson registrant requirements.

Upon meeting specified criteria the DOJ will forward information to NCIC's corollary file, the National Sex Offender Registry (NSOR) on: 1) registered sex offenders with valid addresses; 2) those known to have been deported; 3) those identified as transients; and 4) registered sex offenders whose whereabouts are unknown. Manual criminal history records and the Automated Criminal History System (ACHS) are no longer updated with the registrant's address information. Only the initial requirement to register will be on the ACHS and manual rap sheets. The ACHS displays the message: "FOR CURRENT REGISTRANT ADDRESS INFORMATION INQUIRE INTO THE VCIN SYSTEM."

The VCIN has created an Intranet application featuring an expanded on-line search capability available only to the law enforcement community. The public site available over the Internet at <http://MegansLaw.ca.gov> allows searches by name, address, city ZIP Code, county, parks and schools. The law enforcement Intranet application at <http://167.10.34.34> allows for searches of the sex offender database by offender category, date of birth, Sexually Violent Predator designation, scars, marks and tattoos and other physical and numerical identifiers. Agencies should continue to access VCIN for more comprehensive data, including an offender's registration history, vehicle information and prior addresses.

The Megan's Law Internet site has added a feature that will allow the public to report information about registered sex offenders directly to the DOJ, which will then be forwarded to the appropriate local law enforcement agency. Each sex offender profile includes a "Report Information to DOJ" button. When a user clicks on the button, they are sent to a screen that allows them to provide information about that offender. The screen is prepopulated with identifying information about the offender.

Four categories are identified in determining who will be posted on the Megan's Law Internet site: "Full Address", "ZIP Code Only", "No Post" and Excluded". "Full Address" registrants will have their full residence address displayed on the Internet, whereas "ZIP Code Only" registrants do not meet the criteria for full residence address display. Current law allows certain persons to apply for and be granted an exclusion from disclosure on the site. "No Post" and "Excluded" offenders are not disclosed to the public on the Internet, but are available to law enforcement via the Intranet application.

J. STOLEN VEHICLE SYSTEM (SVS)

Records of stolen, lost, felony, found or evidence vehicles, parts and/or plates are entered by law enforcement into the SVS. Additionally, there are records for pawned, impounded, stored, repossessed and missing person vehicles. An inquiry into this system may be made using the license number (LIC), vehicle identification number (VIN), engine number (ENG), serial number (SER),

owner applied number (OAN) or the file control number (FCN). Most inquiries into SVS are made with only the license plate number. Inquiries made using the VIN will automatically be forwarded to NCIC. When making an inquiry on an out-of-state license, it is necessary to use the license state field (LIS). When there is no exact match to the LIC, VIN, ENG or OAN inquiry, a Near Miss response may be received. Thoroughly research this response by inquiring in the FCN to compare data before taking any action on the Near Miss response.

Expired stolen license plate records, expired stolen boat registration records and expired license plate records for vehicles associated with a missing person will remain in the NCIC License Plate File, Boat File and Missing Persons File for the year of entry plus four years.

When encountering a DOJ STOP or RESTRAINT in the response to a DMV inquiry, check the SVS to determine if the vehicle is still an outstanding stolen. The SVS may have more timely information than the DMV does. If you encounter a DOJ STOP or RESTRAINT on a vehicle which you know to be recovered, contact the Stolen Vehicle Unit at (916) 227-3686.

Three files containing stolen vehicle, felony vehicle and stolen license plate data to assist agencies employing License Plate Reader (LPR) technology are available. The data in these files can be downloaded into mobile or static LPRs with the capability of scanning vehicle license plate numbers in the field and comparing them with known stolen vehicles, felony vehicles or stolen license plates derived from the SVS. Any matches from this downloaded data must be verified against the SVS. The downloads are available from the California Law Enforcement Web (CLEW) site at <http://clew.doj.ca.gov>

Regarding vehicles located in Mexico: The Texas Department of Public Safety's Border Auto Theft Information Center (BATIC) located in El Paso, Texas serves as a liaison between the Mexican and United States (US) police authorities for locating and recovering stolen vehicles. In addition to working with the Mexican officials in recovering US stolen vehicles that are located in Mexico, they are able to obtain information on vehicles registered in Mexico, and check for stolen status of vehicles stolen in Mexico and brought into the US. BATIC will inquire on a vehicle that is located in Mexico, a hit confirmation teletype is sent to the entering agency to determine if the vehicle is the same and whether it is still an active case. The message also states that a "**LOCATE WILL NOT BE PLACED**" on the record at this time, with the instruction *****DO NOT REMOVE FROM NCIC*****. The vehicle is not in the possession of US authorities, and removal from NCIC may interfere with the return of the vehicle via the treaty process. The remarks section of the hit confirmation message will vary in details and information within the body of the text. Please read the text thoroughly. Refer to the CJIS manual SVS section 1.7.1.

K. AUTOMATED BOAT SYSTEM (ABS)

The ABS contains records of boats and boat parts that are stolen, lost, repossessed and /or stored. In 2007, a new boat record type was added for Pawned Boats. Inquiries into the ABS may be made using the registration number (REG), boat hull number (BHN), engine number (ENG), serial number (SER), owner applied number (OAN), Coast Guard Document number (CGN), or FCN. California registered boats have CF as the first two characters of the REG. Inquiries which use the REG or BHN are forwarded to the NCIC Stolen Boat File. Inquiries which use ENG or OAN are forwarded to NCIC as BHN. As with vehicles, a Near Miss response may be received when there is no exact match. Thoroughly research this response by inquiring on the FCN to compare data before taking any action on the Near Miss response. To determine the name of the registered owner of a boat, use the DMV Vessel Registration File. (*DOJ Information Bulletin 07-07-BCIA*)

When a stolen boat entry is accepted by ABS, a stop is placed on the corresponding boat record in the DMV. This DOJ STOP or RESTRAINT is intended to prevent the registration of stolen boats.

When encountering a DOJ STOP or RESTRAINT in the response to a DMV inquiry, check the ABS to determine if the boat is still an outstanding stolen. The ABS may have more timely information than the DMV does. If you encounter a DOJ STOP or RESTRAINT on a boat which you know to be recovered, contact the Stolen Vehicle Unit at (916) 227-3686.

L. AUTOMATED PROPERTY SYSTEM (APS)

The APS is a file of records of serialized property reported as stolen, lost, found, held as evidence, under observation, pawned/bought, and displaying either the manufacturer's and/or owner applied numbers. It also includes non-serialized property that has been uniquely inscribed. Effective July 2007, the APS began accepting all reported "types" of Credit Cards - previously the APS only accepted credit cards reported as stolen. Credit card records are not forwarded to NCIC. Inquiries may be made using the FCN, SER, OAN, or OCA, and either the Type or Brand. Inquiries using SER or OAN with TYP will be forwarded to NCIC. Inquiries can also be made on the subject's name for serialized and non-serialized pawn/buy transactions. Name searches can be conducted by county or statewide, using city/county codes. Use the NCIC Securities File to inquire on securities, as securities are not entered in the APS.

The APS tables are updated on a daily basis and are available for download on the CLEW Web site at <http://clew.doj.ca.gov>. The ABC (Article/Brand/Category) guide is updated on a quarterly basis and also available on CLEW.

M. AUTOMATED FIREARMS SYSTEM (AFS)

The AFS is a file of firearm records pertaining to serialized weapons (such as stolen, lost, and found), as well as, records of weapons associated with the names of persons (such as Dealer's Record Of Sale [DROS], pawned, and voluntary registration/firearm ownership). Records are maintained in two segments, historical and law enforcement. The historical segment contains firearms data that are linked to a specific individual. Records maintained in the law enforcement segment of AFS contain data on firearms generally not associated to any specific individual. Long guns are not maintained in AFS unless they have been reported lost, stolen, found, under observation, retained for official use or voluntary registration. Inquiries into the AFS may be made using the subject's name or the weapons serial number. Only serial number inquiries are forwarded to NCIC. Stolen and Found firearms records may be entered into AFS only (ENT/1), or they may be entered into both the AFS and NCIC Gun Files (ENT/2). Effective April 4, 2008, changes were made to AFS to also allow Lost records to be entered simultaneously in AFS and NCIC using ENT/2. (*DOJ Information Bulletin 2008-BOF-04*)

PC section 12021.3 requires any person who claims title to any firearm that is in the custody or control of a court or law enforcement agency, and who wishes to have the firearm returned, shall submit a Law Enforcement Gun Release Application form to the DOJ to determine eligibility to possess the firearm. The DOJ no longer notifies the custodial agency of the approval. The applicant will be provided with an eligibility letter having a gold Attorney General seal sticker affixed to the letter to present to the custodial agency. Agencies should still check the AFS to determine if the firearm has been reported stolen, that any firearm that is a handgun has been reported in AFS in the name of the individual seeking return of the firearm, and the firearm is otherwise lawful (e.g. not an unregistered assault weapon). DOJ's role is to conduct a firearms eligibility check on the applicant, not to determine whether the particular firearm is legal to be possessed or released to the applicant.

N. MENTAL HEALTH FIREARMS PROHIBITION SYSTEM (MHFPS)

The MHFPS is an inquiry only database containing firearms eligibility information on persons prohibited from owning or possessing firearms due to a mental health disorder per 8100/8103 of the Welfare and Institutions Code (WIC). A response from the MHFPS will indicate personal descriptor information and that the person may be subject to a Mental Health Firearms Prohibition. Access and use of the MHFPS is restricted by WIC sections 8103(e) (3) and 8105(d), which states in part that all information shall be kept confidential. Further information regarding the person may be obtained by contacting the DOJ directly. The MHFPS may be accessed via CLETS, by agencies currently authorized to receive criminal history information, only to determine if a subject of a criminal investigation which involves the acquisition/possession of a firearm, explosive or destructive device by that subject, is eligible to acquire/possess such a device. It shall be used only to determine eligibility. The discretion/authority to use MHFPS to determine firearms eligibility for other non-criminal investigations (e.g., DROS, firearms related licenses/permits, voluntary registrations/firearm ownership, etc.) rests solely with the DOJ. Any person who knowingly furnishes that information for any other purpose is guilty of a misdemeanor. Like the criminal history system, inquiries into MHFPS require a stated purpose and are subject to audit. The route (RTE) field is mandatory.

O. ARMED PROHIBITED PERSONS SYSTEM (APPS)

The APPS houses information on persons who purchased or acquired a handgun(s) on or after January 1, 1996, or registered an assault weapon(s), and subsequently became prohibited from owning and/or possessing firearms under state or federal law. The APPS is a preemptive crime fighting tool for criminal justice agencies statewide. Use of the system will enable identification of, and proper response to, unlawfully armed individuals. Peace officers in the field can use the data to disarm dangerous criminals and others prohibited from owning/possessing firearms. Courts and district attorneys may use data to facilitate informed decisions necessary to disarm subjects during hearings relative to protective orders, parole/probation and/or sentencing proceedings. Direct access is allowed through APPS using message keys QYP (Query Personal Data Record), QYN (Query ID Number) and QYG (Query Gun Serial Number). An agency contact name and telephone number are required when submitting a QYN inquiry to APPS. Agencies with access to the SRF are granted automatic access to the APPS. The SRF QVC query has been enhanced to provide an option to access APPS in addition to the WPS, the CARPOS, and SRF. Query the SRF QVC using the name, sex, date of birth or age, and enter code "Y" for yes or "N" for no in the APP/Data Field. Responses will provide personal data for prohibited persons only and will appear at the end of the QVC response. Agencies should not arrest based solely on a positive response. (*DOJ Information Bulletin 2007-BF-03*)

P. AUTOMATED ARCHIVE SYSTEM (AAS)

The DOJ offers the ability to electronically retrieve Fingerprint Cards transmitted and/or processed electronically through the CAL-ID Automated Fingerprint Identification System and stored as images. The AAS also includes other associated criminal history documents, such as Dispositions of Arrest and Court Actions and Miscellaneous Documents, which have been electronically processed and/or stored.

Q. DEPARTMENT OF MOTOR VEHICLES (DMV)

DMV information obtained via CLETS is confidential and for law enforcement use only.

California Vehicle Code (CVC) section 1808.47 states that any person who has access to confidential or restricted information from the DMV shall establish procedures to protect the confidentiality of those records. DMV records are to be accessed in the course of official business and not for curiosity purposes. Authorized personnel shall not inquire into their own record or have someone inquire for them. According to CLETS policy, periodic driver license checks may be conducted by agencies on employees where driving is a requirement of their job. Home address information must remain in the employee's personnel file and may not be disclosed for any reason (CVC section 1808.45).

Automated files for driver license and identification cards, vehicle and vessel registrations, parking and toll violation information, occupational licensing, and international registration plans are maintained by the DMV and accessible through CLETS. The DMV Driver License/Identification Card (DL/ID) database maintains automated records of California licensed drivers, unlicensed drivers, and those persons who have been issued a CA Identification (ID) Card. Additionally, the DL/ID database contains index records, known as X records, which are established when the DMV receives information from courts and/or law enforcement that cannot be matched to an existing record. There is no photo, thumb print or physical description on file for an X record, therefore the convictions and accidents associated with these records are not verified. The DL/ID database is available for inquiry by DL/ID number, or by name. For name inquiries, the last name is matched by a sound alike system, but the Automated Name Index requires the first name must be spelled exactly as it appears on the driver's license. For example, when running a California Driver's License by name, if the inquiry is on the first name of DEBRA, you will not get a positive response if the first name on record appears as DEBORAH. The DL file is composed of a subject's basic record, identifying information, status of driving privilege, legal history, records of accidents, abstract of conviction, and endorsements and certificates. DMV Information Codes allow access to the entire record or specified parts of the record. There is also a User-Friendly response providing driver records with an easy-to-read and understandable printout.

The DMV maintains an ongoing record of vehicle or vessel ownership. This file includes all vehicle and vessels registered or with planned non-operational status. Records initially established by input from original registrations are updated by renewals, changes of address, and transfers. Parking, toll evasion, owner responsibility citations, and delinquent property taxes on vessels become part of these records temporarily, if left unpaid. The information stored includes the license plate number, vessel CF number, the hull identification number or VIN, description of the vehicle or vessel, name and address of the registered owner, lessee, lessor, and if present, the legal owner.

A series of flags display to alert both law enforcement and the DMV to possible stolen or felony vehicles and stolen boats. These flags are intended to prevent false re-registration and/or transfer of title. Flags are programmatically created, and may be set on DMV vehicle records after an entry is placed on a stolen or felony vehicle in the DOJ Stolen Vehicle System, depending on the data elements entered.

The vehicle flags may be either a DOJ STOP, DOJ RESTRAINT, or DOJ REFERRAL. The flag for a stolen vessel will be a DOJ RESTRAINT. Do not rely solely on the DMV response to determine if a vehicle or vessel is stolen. Always verify with an inquiry into the Stolen Vehicle or Automated Boat System.

All insurance companies issuing private passenger automobile liability policies in California are required to electronically report policy information to the DMV's insurance database. The DMV will use this information to display a status indicator on CLETS inquiries and vehicle registration

printouts. The information will appear below the Date and Time fields, and will follow a “DOJ STOP” notice, if present. The flags will indicate if the insurance information is on file, unknown, unavailable or pending. (*DMV Law Enforcement Information Memo 06-02*)

R. NATIONAL CRIME INFORMATION CENTER (NCIC)

The following files are available from NCIC:

Interstate Identification Index	Boat File
Wanted Person File	Article File
Protection Order File	Gun File
Supervised Release File	Securities File
Missing Person File	Foreign Fugitive File
Unidentified Person File	US Secret Service Protective File
Convicted Sexual Offender Registry File	Violent Gang and Terrorist Organization File
Vehicle File	ORI File
License Plate File	Identity Theft File
Vehicle/Boat Parts File	Immigration Violator File

The NCIC system is nationwide computerized information system serving all 50 states, the District of Columbia, the Commonwealth of Puerto Rico, the U.S. Virgin Islands, and Canada. The NCIC system stores vast amounts of criminal justice information. It can best be described as a computerized index of documented criminal justice information concerning crimes and criminals of nationwide interest. A name inquiry through California’s Wanted Persons System or Supervised Release File, with a numeric identifier such as date of birth, will automatically be forwarded to NCIC for a search of not only their Wanted Persons File, but all their files that have records stored by name (excluding the III). These include: Missing Person File, Immigration Violators File, Protection Order File, Convicted Sexual Offender Registry, U.S. Secret Service Protective File, Foreign Fugitive File, Supervised Release File, Gang/Terrorist Files, and Identity Theft File. Matches are made in these NCIC files based on a phonetic encoding of the last name and an exact match of the DOB. Similarly, a SVS inquiry with an out-of-state license plate or VIN, not only searches the NCIC Stolen Vehicle File but also the License Plate File. NCIC has made a programmatic change to disregard the license plate state (LIS) and search only the license plate number (LIC) for felony vehicle records when an agency makes an inquiry using both the LIC and LIS fields. A caveat will advise the match is based on an LIC search only (not the LIS) and that all data should be verified before taking any further action.

The Terrorist Screening Center has requested the FBI modify the Violent Gang and Terrorist Organization File (VGTOF) caveats to emphasize to law enforcement agencies they should not advise subjects that they are included on the terrorist watch lists. VGTOF information is exclusively for the use of criminal justice agencies and shall not be disseminated to a noncriminal justice agency or the subject.

The Identity Theft File (ITF) serves as a means for law enforcement to flag stolen identities and acknowledge the victim. The victim reports the loss or theft and fraudulent use or intent to use to a law enforcement agency. Information entered will create a victim profile that is made readily available to law enforcement during future encounters, such as routine traffic stops. The victim will be provided with a password by the ITF to document their report of identity theft.

The Interstate Identification Index (III) is an automated system which serves as a pointer to automated criminal history records maintained by the FBI and all 50 states. Records of individuals with a year of

birth of 1956 or later, or persons arrested for the first time on or after July 1, 1974, regardless of their dates of birth, are indexed in III. An initial query uses the name, sex, date of birth and race (NCIC race codes only). When a complete date of birth is used, the search will provide records that are based on matching name, sex, race, and date of birth (plus or minus 3 years on the year of birth). If a positive response is received, a subsequent query using the FBI number or State Identification Number (SID) should be initiated to retrieve the record(s). More than one state may respond with a record. However, not all states have all of their automated criminal history records indexed in III. Some states, like California, may have some automated records not indexed in III, as well as some manual records or hybrid records, etc. A subsequent search directly into a state not providing an III response should be conducted utilizing the National Law Enforcement Telecommunications System (NLETS) criminal history inquiry formats (CHRI queries IQ/AQ/FQ).

A rap sheet returned from California's Automated Criminal History System will have a comment regarding III records indicating the subject has a record in the III pointing to California only or the subject has a record in III pointing to California and another state(s) and/or to the FBI files. Even so, it is best to follow up with an III inquiry and consider inquiring directly to any state using the NLETS formats if you have information that the subject has been in that state.

Note: Agencies with CLETS access are no longer authorized to query the Interstate Identification Index to obtain criminal history information via Purpose Code X transactions for a child welfare agency. Child welfare agencies still may secure California criminal history information via law enforcement agency use of CLETS for the existing reasons listed in Welfare and Institutions Code section 16504.5.

An NCIC off-line search is a special technique used to obtain information from NCIC that can not be obtained from an on-line inquiry. An off-line search of the NCIC transaction log will reveal whether inquiries were made on a particular individual or property item (i.e. during a traffic stop) for a specified time frame, even if no match was returned. From an off-line search of purged records, it can be determined if a property item theft was entered and subsequently removed due to its retention expiration, even though an on-line inquiry produces a "NO RECORD" response. An off-line search of active records can also be performed using descriptive information. Contact the NCIC Investigation and Operational Assistance Unit at (304) 625-3000, or send an Administrative Message through NLETS to the ORI of DCFBIWAQ9.

S. NATIONAL LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEM (NLETS)

The NLETS is a computerized, high speed message switching system created for and dedicated to the criminal justice community. Its sole purpose is to provide for the interstate and/or interagency exchange of criminal justice-related information. One method of communication would be an Administrative Message sent as a State or Regional Broadcast. Administrative Messages are sent to an agency's nine-character ORI, whereas regional broadcasts are sent to a two-character code. Up to five addresses are allowed in an NLETS Administrative Message. NLETS also allows users the ability to retrieve information from NLETS supported systems and files such as: Hazardous Material (HAZMAT), ORI On-line (ORION), International Police Organization (INTERPOL), the National Insurance Crime Bureau (NICB), NLETS Help files and an interface with the Canadian Police Information Centre (CPIC) files. CPIC is a system similar to NCIC, providing wanted and stolen files and vehicle registration and driver license information. The ORION file allows a search for law enforcement and criminal justice agency information (address, phone, fax, hour of operation, etc.) by Location (city or county) or ORI. In addition, NLETS supports direct inquiries into state motor vehicle, drivers' license, criminal history and other state databases. The initial query for criminal history records should always start with the NCIC Interstate Identification Index. However, not all

automated criminal history records are indexed in the III, nor are manual records included. NLETS Criminal History Record Information should be used as a supplement, not a substitute, to NCIC's III. When Race is included in your inquiry, use the NCIC Race Codes of A (Asian), B (Black), I (Indian), W (White) and U (Unknown).

Effective October 2008, the California DOJ and INTERPOL's United States National Central Bureau (USNCB) added six new message keys allowing authorized NLETS users the ability to access INTERPOL data via the Automated Search Facility (ASF). These message keys allow agencies to run queries against wanted person, stolen vehicle, or stolen travel document files, returning all negative and positive responses, including additional relevant information. A positive full inquiry hit generates a pre-formatted message containing mandatory handling instructions to validate the information with the country of origin. (*DOJ Information Bulletin 08-09-BCIA*)

NLETS has additional information and some recently added files, some of which each state may or may not support including: Parole, Probation, Corrections Transactions; Sex Offender Registration Transactions; FAA/TECS Aircraft Tracking and Registration System; Road/Weather Transactions; Commercial Vehicle Information; International Fuel Tax Association; National Drug Pointer Index; Concealed Weapons Permit Information; Wildlife Violation File; and Mexican Licenses.

T. OREGON LAW ENFORCEMENT DATA SYSTEM (LEDS)

The computer interface with the Oregon LEDS allows CLETS users direct inquiry to the Oregon Vehicle Registration, Driver's License, Stolen Vehicle, Wanted Persons, Restraining/Protection Order, Gun, and Article files. The direct interface with Oregon provides CLETS users more complete and timely information than is available from inquiries via NCIC or NLETS. Oregon criminal history inquiries and administrative messages must be routed through NLETS.

REMEMBER, a computer match on a person or property is not probable cause for arrest or confiscation in and of itself. CONFIRMATION is required.

RESOURCE MATERIAL

CJIS Operating Manual – Rev. varies 09/08/97–12/08
NCIC Operating Manual – Rev. 09/08
NLETS User and Technical Guide – Rev. 01/01/08
CLETS Operating Manual – Rev. March 1998
CLETS Policies, Practices and Procedures – Rev. 02/09
DMV Manual for CLETS – Rev. June 2008
California Penal Code
California Vehicle Code
California Code of Regulations
DOJ Information Bulletins

SECTION ONE
FULL ACCESS AND LESS THAN FULL ACCESS OPERATOR
COMBINED WORKBOOK QUESTIONS

Name: _____

Date: _____

Score: _____

(70% Passing Score Acceptable)

GENERAL POLICIES AND LIABILITY/SECURITY ISSUES

1. Personnel shall not operate or have access to the CLETS terminals, equipment or information until a background and fingerprint check is _____.
 - A. Started
 - B. Completed
 - C. In progress
 - D. All of the above

2. In order to verify the accuracy of information in the Automated Firearms System or the Department of Motor Vehicles, an individual is allowed to inquire into their own record.
 - A. True
 - B. False

CALIFORNIA LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEM (CLETS)

3. A computer match on a person or property is probable cause for arrest or confiscation in and of itself.
 - A. True
 - B. False

4. What must an agency access in order to confirm a hit on the originating agency's person or property?
 - A. All Points Bulletin
 - B. The originating agency's Master Case Record
 - C. The appropriate automated CJIS database
 - D. All of the above

CRIMINAL JUSTICE INFORMATION SYSTEM (CJIS)

CRIMINAL HISTORY SYSTEM (CHS)

5. A preliminary record check may be performed on any person prior to their approval as a “ride-along” with a law enforcement officer, provided that person is not an employee of the law enforcement agency.
 - A. True
 - B. False

6. Penal Code section 11142 states that any person who is authorized by law to receive a record who knowingly furnishes the record to a person not authorized is guilty of a _____.
 - A. Infraction
 - B. Misdemeanor
 - C. Felony
 - D. All of the above
 - E. None of the above

7. Law enforcement agencies are authorized to access CORI through the CLETS for licensing, employment and/or certification.
 - A. True
 - B. False

8. _____ will indicate the criminal history record is not based on fingerprint identification.
 - A. ASP
 - B. APP
 - C. DSP
 - D. None of the above

9. What is required for all ACHS inquiries via the CLETS?
 - A. Authorized purpose
 - B. Operator ID and Requestor ID if different than Operator
 - C. Right-to-know
 - D. All of the above

WANTED PERSONS SYSTEM (WPS)

10. The NCIC policy requires what contact method be used for all hit confirmation requests?
 - A. Telephone
 - B. YQ and YR transactions
 - C. FAX
 - D. E-mail
 - E. All of the above

11. A warrant entered as ENT/2 means:
- A. The warrant is in CA only
 - B. The agency is not willing to extradite
 - C. The warrant is in the NCIC only
 - D. The warrant is in CA and the NCIC
12. The CLETS will forward a WPS inquiry to the NCIC when _____ is included.
- A. Name and Sex
 - B. Name, Sex and Date of Birth
 - C. Name, Race and Numeric Identifier
 - D. Name, Race and Vehicle Identifier

CALIFORNIA RESTRAINING AND PROTECTIVE ORDER SYSTEM (CARPOS)

13. Any agency with inquiry only capabilities into the CARPOS is able to add a violation message to an existing restraining order record.
- A. True
 - B. False

SUPERVISED RELEASE FILE (SRF)

14. The SRF provides for a two-way communication link which allows inquiring law enforcement officers to send information about an encounter with a subject to the agency that entered the record. This is called the:
- A. Supporting documentation
 - B. Master Case Record
 - C. Hit Confirmation
 - D. Contact Message
15. What information can be placed in a Contact Message by an agency making an encounter with a parolee, probationer, registrant, etc.?
- A. Type of encounter (Routine, Booking, Citation)
 - B. Vehicle information
 - C. Date, time and location of contact
 - D. All of the above
16. Which of the conditions below is required for a supervising agency to receive a Notice of Arrest from the DOJ?
- A. The subject's SRF record contains the subject's CII number
 - B. A Contact Message has come in
 - C. An arrest print has been updated to the subject's criminal history record
 - D. A and C above
 - E. All of the above

MISSING AND UNIDENTIFIED PERSONS SYSTEM (MUPS)

17. Law enforcement does not have to accept a missing person report over the telephone.
- A. True
 - B. False
18. An All Points Bulletin sent to group code 4500 for a Child Abduction Alert will be broadcast statewide, and can be initiated whether or not the abduction meets the Amber Alert criteria.
- A. True
 - B. False
19. The Unidentified Persons System may contain records of either deceased or living individuals, as well as body parts.
- A. True
 - B. False

SEX AND ARSON REGISTRATION (SAR)

VIOLENT CRIME INFORMATION NETWORK (VCIN)

20. The Sex and Arson Registration records containing all registration history, compliance status, and address information is available from which system:
- A. The ACHS rap sheet
 - B. Supervised Release File
 - C. Violent Crime Information Network
 - D. All of the above
21. The VCIN has created an Intranet application featuring an expanded on-line search capability available only to the law enforcement community.
- A. True
 - B. False

STOLEN VEHICLE SYSTEM (SVS)

22. What data is available to agencies employing License Plate Reader technology for downloading to mobile terminals?
- A. Stolen vehicle
 - B. Felony vehicle
 - C. Stolen license plates
 - D. All of the above

23. What agency acts as a liaison between the Mexican and US police authorities for locating and recovering stolen vehicles from Mexico?
- A. US Customs and Border Patrol
 - B. The Texas Department of Public Safety's BATIC
 - C. The National Auto Theft Bureau

AUTOMATED BOAT SYSTEM (ABS)

24. Which database would you inquire to determine the registered owner of a boat?
- A. The ABS
 - B. The DMV Vessel Registration File
 - C. Both A and B
25. Contact the _____ if you encounter a DOJ RESTRAINT on a boat that is known to be recovered.
- A. DMV
 - B. National Insurance Crime Bureau
 - C. The DOJ SVS Unit at 916-227-3686
 - D. All of the above

AUTOMATED PROPERTY SYSTEM (APS)

26. What types of property are found in the APS?
- A. Serialized property
 - B. Non-serialized property with unique inscriptions
 - C. Lost credit cards
 - D. Securities
 - E. A, B and C above

AUTOMATED FIREARMS SYSTEM (AFS)

27. Inquiries made on the _____ will forward to the NCIC:
- A. Subject's name
 - B. Serial number
 - C. Both subject's name and serial number
28. Prior to the release of a weapon, should agencies run an AFS name inquiry on individuals even if they present a DOJ Law Enforcement Gun Release eligibility letter?
- A. Yes
 - B. No

MENTAL HEALTH FIREARMS PROHIBITION SYSTEM (MHFPS)

29. What type of information can be obtained in the MHFPS?
- A. Persons prohibited from owning firearms per the WIC
 - B. Personal descriptor information
 - C. Persons prohibited from possessing firearms per the WIC
 - D. All of the above.
30. The Welfare and Institutions Code restricts access into the MHFPS to what purpose?
- A. When doing background checks on peace officer applicants and political candidates
 - B. To determine if a person who is the subject of a criminal investigation which involves the acquisition/possession of a firearm, explosive or destructive device by that person, is eligible to acquire/possess such a device
 - C. Prior to entering a "Firearm Ownership" record into the AFS
 - D. All the above

ARMED PROHIBITED PERSONS SYSTEM (APPS)

31. What data fields are required when submitting a QYN inquiry to the APPS.
- A. Agency contact name
 - B. Agency CLETS Coordinator's telephone number
 - C. Agency telephone number
 - D. A and C above
32. Other than an APPS direct inquiry, what other CJIS database(s) will allow you access to the APPS?
- A. Automated Firearms System
 - B. Wanted Persons System
 - C. Supervised Release File
 - D. All of the above

AUTOMATED ARCHIVE SYSTEM (AAS)

33. The AAS can be accessed to provide digital images of what information?
- A. Fingerprint cards
 - B. Disposition of Arrest and Court Actions
 - C. Miscellaneous Documents
 - D. All of the above

DEPARTMENT OF MOTOR VEHICLES (DMV)

34. Periodic driver license checks may be conducted by agencies on employees where driving is a requirement of their job.
- A. True
 - B. False
35. Automated Name Index queries require the driver's first name to be identical to the DMV record.
- A. True
 - B. False
36. What is the purpose of a DOJ STOP, RESTRAINT or REFERRAL flag, and what should an agency do when encountering one in response to a DMV inquiry?
- A. It means nothing – ignore the response
 - B. It is meant to prevent the registration of a stolen vehicle or boat - check the SVS or the ABS to determine if the vehicle or boat is still an outstanding stolen

NATIONAL CRIME INFORMATION CENTER (NCIC)

37. A name inquiry into the DOJ's Wanted Persons System will be forwarded to the NCIC for a search of all their persons files, only if what information is included in the inquiry?
- A. Race
 - B. Height
 - C. Date of birth or other numeric identifier
 - D. All of the above
38. A vehicle query forwarded to the NCIC with the License Plate State and the License Plate Number will return matches of felony vehicles that have been searched against both the licensing state and plate number.
- A. True
 - B. False
39. A "no record" response for III means there is absolutely no record in any of the 50 states.
- A. True
 - B. False

NATIONAL LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEM (NLETS)

40. The ORION file provides responses for an inquiry by:
- A. Location (city or county)
 - B. Originating Agency Identifier (ORI)
 - C. Mnemonics
 - D. A and B

41. The NLETS supports direct inquiries into what types of state files?
- A. Motor vehicles
 - B. Drivers' license
 - C. Criminal history
 - D. All of the above
42. The NLETS Criminal History Record Information can be used as a substitution for the Interstate Identification Index.
- A. True
 - B. False
43. Which Race codes should be used in an NLETS inquiry?
- A. DOJ Race Codes
 - B. NCIC Race Codes
 - C. NASCAR Race Codes
 - D. None of the above
44. Access to INTERPOL records via the NLETS provides information on international wanted persons, stolen vehicles, and stolen travel documents.
- A. True
 - B. False

OREGON'S LAW ENFORCEMENT DATA SYSTEM (LEDS)

45. The computer interface with Oregon LEDS allows CLETS users direct inquiry into which files?
- A. The Oregon Vehicle Registration, Driver's License, Stolen Vehicle, Wanted Persons, Restraining/Protection Order, Gun and Article files
 - B. Only the Drivers License and Wanted Persons
 - C. Only the Stolen Vehicle and Drivers License
 - D. Only the Wanted Persons and Gun File

SECTION TWO
FULL ACCESS OPERATOR WORKBOOK
COMPLETION LOG

Employee Name: _____

The Agency CLETS Coordinator (ACC) or supervisor administering the training must date and initial each completed chapter. All operators must complete Chapters A, B and C, and then only those databases pertinent to their job assignments. Employees should maintain a copy of this log for their records.

CHAPTER	COMPLETION DATE	INITIALS
A. General Policies and Liability/Security Issues		
B. Record Maintenance Responsibilities		
Criminal Justice Information Systems (CJIS)		
C. Wanted Persons System (WPS)		
D. California Restraining and Protective Order System (CARPOS)		
E. Supervised Release File (SRF)		
F. Missing and Unidentified Persons System (MUPS)		
G. Sex and Arson Registration (SAR) - Violent Crime Information Network (VCIN)		
H. Stolen Vehicle System (SVS)		
I. Automated Boat System (ABS)		
J. Automated Property System (APS)		
K. Automated Firearms System (AFS)		
National Crime Information Center (NCIC)		
L. Identity Theft File (ITF)		
M. Securities File		
N. Violent Gang Terrorist Organization File (VGTOF)		

SECTION TWO

FULL ACCESS OPERATOR WORKBOOK

A. GENERAL POLICIES AND LIABILITY SECURITY ISSUES

Any information accessed via CLETS is confidential and for official use only. Access is defined as the ability to hear or view any information provided through CLETS. It is required that each employee/volunteer sign an employee statement form prior to operating or having access to CLETS terminals, equipment, or information. This form addresses confidentiality, release, and misuse of CLETS information. When an agency determines CLETS information is no longer needed, the information and/or systems records shall be securely disposed of to prevent access by unauthorized personnel.

B. RECORD MAINTENANCE RESPONSIBILITIES

At the time of entry, you may elect to enter a record into California's Criminal Justice Information System (CJIS) only or into both CJIS and the National Crime Information Center (NCIC). All entries into the Missing and Unidentified Persons System (MUPS) are automatically forwarded to NCIC. In order for a record to be accepted by NCIC, it must meet NCIC entry criteria. Otherwise, depending on the CJIS system, the record will either be rejected by NCIC or not forwarded from CJIS. Your agency may subsequently remove a record from NCIC but retain it in CJIS by a simple modification (not applicable to MUPS entries). To change a record from CJIS only retention to CJIS and NCIC, the record must be removed from CJIS and re-entered into CJIS and NCIC. An exception is a Wanted Persons System (WPS) record which only needs to be modified for NCIC entry. With the exception of the Securities File, Identity Theft File and Violent Gang Terrorist Organization File, CLETS terminals cannot enter NCIC only records.

The responsibility for the accuracy, timeliness, and completeness of a record residing in a CJIS/NCIC database lies with the agency that entered the record into the system. Each record entered into CJIS and/or NCIC must be based on a Master Case Record maintained by the entering agency. To ensure accuracy and completeness of records, all entries must be double-checked by a second party at the time of entry (second party verification). A "hit" on a person or property record is not probable cause for arrest by itself. The inquiring agency must confirm the warrant or record with the entering agency. The contributing agency of the entry must have the Master Case Record available at all times, and must access the Master Case Record, in order to provide a substantive response to a hit confirmation request within the required response time. (Urgent – 10 minutes or Routine – 1 hour.) A substantive response is defined as either: a) hit confirmed; b) hit denied; or c) a response indicating the agency is unable to respond at this time, but will reply within a specified period of time.

Both the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) require that automated records in selected files be periodically validated by their contributors. Agencies must compare each record on the validation list with its source documents and supplemental reports to ensure all available information, including optional data, has been entered. The contributor must also attempt to consult the appropriate complainant, victim, prosecutor, court, motor vehicle registry files, or other appropriate source or individual, to assure the record is still active. Records which cannot be validated, are inaccurate, or not current, must be removed from the system by the entering agency.

If new data is added to the Master Case Record, you must modify the CJIS record to include the new data, even if it's an optional data field. If data in the CJIS record is incorrect and correct data is

available, you must modify the CJIS record to correct the data. If data in the CJIS record is inaccurate and the correct data is unavailable, and the data is in an optional data field, you must modify the record to delete the data. If the data is in a mandatory field, you must cancel the CJIS record. If the reliability of the Master Case Record is in doubt, you must cancel the CJIS record. If the property of record is recovered, you must clear or cancel the CJIS record (depending on the system). If the subject of a WPS record is apprehended, you must cancel the WPS record. If the Master Case Record is unavailable – CANCEL the CJIS record.

Penal Code (PC) section 11108 requires “each sheriff or police chief executive shall submit descriptions of serialized property, or non-serialized property that has been uniquely inscribed, which has been reported stolen, lost, found, recovered, held for safekeeping, or under observation, directly into the appropriate DOJ automated property system for firearms, stolen bicycles, stolen vehicles, or other property, as the case may be.”

CRIMINAL JUSTICE INFORMATION SYSTEM (CJIS)

C. WANTED PERSONS SYSTEM (WPS)

Enter all available information from your Master Case Record warrant. This is referred to as “packing the record.” If you have the information for an optional data field, enter it. It is easier to identify or discount a subject as being a wanted person when more information is available in the response. Inquiries should be made into the DOJ Master Name Index and the DMV Automated Name Index files to gather complete or additional identifying data for the WPS entry. Caution and Medical Condition (CMC) Codes should be entered to indicate special handling of a person, medical conditions, or to relay vital information for officer safety.

Agencies can place a locate on a record when the subject of a wanted person record entered by another agency has been apprehended and a positive hit confirmation is received. An agency cannot place a locate on its own record. When an agency apprehends its own subject, the record must be canceled by the entering agency. If a locate is entered incorrectly, contact the DOJ Wanted Persons Unit. Only the DOJ can remove a locate from a record.

D. CALIFORNIA RESTRAINING AND PROTECTIVE ORDER SYSTEM (CARPOS)

An agency can enter a restraining/protective order into the CARPOS as long as the agency holds a copy of the order. Only one agency should enter an order into the CARPOS. Do not enter an order if it is already in the CARPOS. Restraining/protective orders are effective on the hearing date or on the date next to the judge’s signature, whichever is the earliest. Mandated orders shall be entered into the CARPOS, whether the order has been served or is unserved. When law enforcement officers encounter the subject of an unserved restraining order, they shall advise the restrained person of the terms of the order and provide the name of the court that issued the order so the restrained person can obtain a copy of the order. Immediately following the service of a restraining order, all service information shall be updated into the CARPOS via CLETS.

The CARPOS contains both active and inactive records. The inactive records, including suspended records and associated violation messages, are maintained in the History file. Once a record expires or is cancelled, it will be held in suspense for 30 days. The originating agency can re-activate a record in a suspended state by modifying the expiration data field to a future date. If the record is not re-activated, on the 31st day it will be deemed a history record and will be stored in the CARPOS history file for an additional five years. Records residing in the history file, including those in suspense, can be accessed by agencies via CLETS using the CARPOS history file query (QRRH).

The CARPOS uses the CLETS headers IB and UB for all Inquiry and Update transactions. Over the years, due to legislation, the number of restraining/protective order types mandated for entry into the CARPOS has increased to 14 types of mandated orders. The most recent types added were the Elder or Dependent Adult Abuse Orders. These orders include both physical and financial abuse. Additionally, in 2008, Family Code section 6380 was amended to allow pets to be included on restraining/protective orders as protected parties.

Regarding “NON-CLETS” ORDERS: If you receive a mandated order on one of the Judicial Council forms and the word “CLETS” has been crossed out, and/or the word “NON-CLETS” has been added to the form, you will still enter the order into the CARPOS. If you have any questions, please contact the CARPOS Unit at (916) 227-6418.

E. SUPERVISED RELEASE FILE (SRF)

The entry of records into the SRF is restricted to specified agencies by record type. Only county and federal probation departments may enter probation records. Only the California Department of Corrections and Rehabilitation (CDCR) and the Division of Juvenile Justice (DJJ) may enter parole records. The Department of Justice (DOJ) Violent Crime Information Network updates SRF twice daily with sex and arson registration data. Only the Department of Mental Health may enter their records. Any police or sheriff’s department may enter Career Criminal records, which are defined in PC section 13853.

The DOJ allows for the entry of selected SRF records into the NCIC SRF for access by law enforcement agencies nationwide. Only Parole, Probation and Mental Health records may be entered as Entry Level (ENT) 2 for transfer to the NCIC SRF. When a supervising parole or probation agency, or DMH designates ENT/2 when entering or modifying a SRF record, the SRF will automatically generate and submit an entry transaction for the NCIC SRF.

The SRF has a full set of tests/training message keys (TMKE’s) to support testing and training activities of agencies using SRF. Agencies that use production message keys to conduct training and testing activities must stop using them and use the TMKE’s instead. Agencies that currently have test and training records entered in the production SRF database should cancel/clear them as soon as possible.

F. MISSING AND UNIDENTIFIED PERSONS SYSTEM (MUPS)

PC section 14205(a) requires all local police and sheriff’s departments to accept any report of a missing person, including runaways, and handle those reports in a priority over property crimes. Information on the missing person must be entered into the Missing Persons System (MPS). If the missing person is at risk or is a child 16 years of age or younger, the missing person record must be entered within four hours. A Be-On-The-Look-Out (BOLO) must also be sent within the reporting agency’s jurisdiction if the missing person is under 16 or at risk. Federal Law Title 42, US Code section 5779(a) requires the immediate entry of all missing persons under the age of 21 in the state and national missing person files. If a missing person case is resolved prior to the entry of the case into MPS, the agency should make an entry, and then immediately cancel the entry. Within 10 days of a child’s disappearance, Education Code sections 49068.6(a), (b), (c), and (d), requires law enforcement to notify the school district, educational agency or private school in which the child is enrolled, that the child is missing. This notification must be in writing with a copy of a photograph, if

available. Photographs and dental X-rays of missing persons should be sent to the MUPS Unit on all open cases.

The MPS allows for the entry of a code (category “K”) indicating an Amber Alert has been issued for the missing person. The record is forwarded to NCIC, which then automatically notifies the National Center for Missing and Exploited Children and the Federal Bureau of Investigation regarding the Amber Alert. In accordance with changes in federal statutes, law enforcement is required to immediately enter records into NCIC for missing juveniles under the age of 21.

The MPS allows for the entry of Suspect and Vehicle data. This is accomplished by entering separate supplemental transactions with their own message keys. As many as three vehicles and suspects can be entered in separate transactions to one record. Entering the required data on a vehicle will cause a Missing Person Vehicle record to be created in the Stolen Vehicle System. Suspect and Vehicle data should not be placed solely in the missing person’s miscellaneous (MIS) field, as the MIS field is not searchable.

The law enforcement agency investigating the death of an unidentified person shall report the death to the DOJ no later than ten days after the date the body or human remains were discovered. If partial body parts are found and identified as that of a missing person, do not cancel the missing person record. Modify the record’s MIS field with this information, thereby allowing the record to remain active should additional body parts be found for future matches.

G. SEX AND ARSON REGISTRATION (SAR) – VIOLENT CRIME INFORMATION NETWORK (VCIN)

Records that are entered into VCIN by law enforcement are retained indefinitely, unless an individual registrant is deceased or has been found that he/she is no longer required to register per court documentation. Since sex and arson registration is a lifetime requirement and VCIN is a relational database, all law enforcement agencies with CLETS capability may contribute information to a registrant’s record. The common goal is to have one record in VCIN on a registrant and that the information is entered/updated in a timely and accurate manner. If an individual has registered with one agency, and then subsequently moves to another agency’s jurisdiction, the new agency should modify the existing registration record to show ownership of the record, and not create an additional sex registration record.

Supporting registration documents should be retained by the entering/updating agency and available at all times. Documentation may be called into court.

Generally, sex offenders must register annually within five working days of their birthday, when moving to a new jurisdiction or when changing their address. Arson registrants must register within fourteen days of entering an agency’s jurisdiction or changing their address. If a registration record is located in VCIN and the inquiry response indicates “DOJ FP CARD REQUIRED”, update VCIN with the registration information, and then mail a completed registration fingerprint card to the Sex Offender Tracking Program (SOTP). If the response indicates, “DOJ FP CARD NOT REQUIRED,” update VCIN with the registration information and keep the registration documentation in your agency files. Registration fingerprints and updates may now be submitted via the Livescan process. (*DOJ Information Bulletin 07-11-BCIA*)

A photograph for a first-time registrant or an offender updating his/her annual registration should be taken and submitted to the SOTP. Sex registrants enrolled or employed at an institution of higher learning have an obligation to register with the police department that has jurisdiction over the

campus. A registrant must notify and provide their new address to the last registering agency, in person, when they plan to move. If the new address is out of their jurisdiction, but still in California, the last registering agency is to update that address into VCIN. This transaction will generate a message to the law enforcement agency having jurisdiction over that new address. The message will advise them of the intention of the registrant relocating to their jurisdiction with the address.

When a registrant notifies the last registering agency that they are moving out of state, or the last registering agency has documentation that the registrant is out of state, VCIN needs to be updated to reflect the out of state status of the registrant. After VCIN is updated, a message will be generated and sent to the state where the registrant resides. When the last registering agency has documentation that shows that the registrant has been deported, VCIN should be updated to reflect this status. For the date of registration, use the date that VCIN is updated and in the MIS field, denote the actual date of deportation. If you know the country where the registrant was deported to, use the country code in the state code field. If the registrant's whereabouts is unknown, after confirmation that the registrant is no longer living at the last registered address, VCIN should be updated to reflect their status as unknown.

Due to the fact that VCIN records share ownership with many agencies, there is no cancel message process. If information is entered or added to an existing VCIN record in error, the user must call SOTP at 916 227-3288 to correct the error. The status of Deceased or Incarcerated can only be entered by the DOJ, by submitting an SS-8102 form to the SOTP.

Because the records of sex offenders are available over the Internet at www.meganslaw.ca.gov, accurate reporting of address and zip code data is crucial. The inclusion of N, S, E, or W, and consistency with street, boulevard, avenue, parkway, etc. is vital. In many localities there is a significant difference between similar addresses, such as 21st Avenue and 21st Street. Also erroneous entry or modification of the subject's birthday may programmatically place him/her "Out of Compliance".

H. STOLEN VEHICLE SYSTEM (SVS)

The California Vehicle Code (CVC) section 10500 and the PC section 11108 requires all serial numbered vehicles, which are reported to a peace officer as taken, stolen, lost, or recovered, and license plates which are reported stolen or lost, be entered into SVS. Other record types such as stored, impounded, repossessed, felony and missing person vehicles (via MUPS) may be placed into SVS. Use the reference (REF) data field to enter the place of vehicle storage and telephone contact information for retrieval of the vehicle for all "stored" and "impounded" vehicle records. A felony vehicle is a vehicle that was involved in the commission of a felony crime, or a vehicle that is subject to seizure based upon a court order (warrant). Vehicle records need not have a license plate number to be entered. However, you should enter "NO PLATES" in the MIS field if the vehicle did not have any at the time of theft (e.g., vehicles stolen from a dealer). When vehicles and/or vehicle parts and/or vessels and/or vessel parts are stolen at the same time and are reported stolen in the same theft or crime report, enter them as a group record. All records must have the same ORI, date of theft (DOT), and agency case number (OCA). Check the DMV Registration File to verify the accuracy of a VIN or to obtain a VIN when there is none in the Master Case Record. If a VIN exceeds 20 characters, enter the last 20 characters in the owner applied number (OAN) field and enter the full VIN in the MIS Field. Entry of a stolen vehicle record into SVS is required even if the vehicle is recovered before the entry is made. In such a case, enter the stolen vehicle record and immediately remove it (i.e. clear the record).

Do not place a locate on vehicles located in Mexico. Refer to the SVS Section 1.7.1 of the CJIS manual. The Texas Department of Public Safety's Border Auto Theft Information Center (BATIC)

located in El Paso, Texas serves as a liaison between the Mexican and United States (US) police authorities for locating and recovering stolen vehicles. In addition to working with the Mexican officials in recovering US stolen vehicles that are located in Mexico, they are able to obtain information on vehicles registered in Mexico, and check for stolen status of vehicles stolen in Mexico and brought into the US. BATIC will inquire on a vehicle that is located in Mexico, a hit confirmation teletype is sent to the entering agency to determine if the vehicle is the same and whether it is still an active case. The message also states that a **“LOCATE WILL NOT BE PLACED”** on the record at this time, with the instruction ***** DO NOT REMOVE FROM NCIC *****. The vehicle is not in the possession of US authorities, and removal from NCIC may interfere with the return of the vehicle via the treaty process. The “remarks” section of the hit confirmation message will vary in details and information within the body of the text. Please read the text thoroughly. Refer to the SVS Section 1.7.1 of the CJIS Manual.

I. AUTOMATED BOAT SYSTEM (ABS)

The DOJ maintains the ABS which contains records of boats and boat parts that are stolen, lost, repossessed and/or stored. In 2007, a new boat record type was added for use with Pawned Boats. The boat pawn transaction number is placed in the OCA data field. Use the victim data fields to enter the name, address and telephone number of the person who pawned the boat. Use the Miscellaneous field to enter the pledger’s ID number, DOB, and the name of the pawnshop.

The California Vehicle Code (CVC) section 10551 requires peace officers to immediately report to the DOJ ABS any reliable report the officer receives regarding stolen or recovered boats. Agencies are required to enter a stolen boat into ABS even if it is recovered before the ABS entry has been made. In such a case, enter the stolen boat record and immediately clear it as being recovered. Stored and repossessed boat record types should be entered to avoid the later entry of erroneous stolen boat records. Embezzled boats may be entered as stolen only if an arrest warrant has been issued for the suspected embezzler CVC section 10553).

J. AUTOMATED PROPERTY SYSTEM (APS)

PC section 11108 requires “each sheriff or police chief executive shall submit descriptions of serialized property, or non-serialized property that has been uniquely inscribed, which has been reported stolen, lost, found, recovered, held for safekeeping, or under observation, directly into the appropriate DOJ automated property system for firearms, stolen bicycles, stolen vehicles, or other property, as the case may be.” To facilitate the entry of non-serialized property, the OAN data field will accept all alpha characters, except for the words NONE or UNKNOWN. Only two Type codes are allowed for non-serialized property to be entered into the APS; Type Code A, for non-serialized jewelry items and Type Code N for all other non-serialized property with valid type codes. The timely entry of all reports of pawn or buy transactions into the APS is vital to the system’s built-in tracking and stolen property recovery capabilities. Additionally, these entries will facilitate the monitoring of individuals whose activities are of interest to law enforcement. If a serial number (SER) or an owner applied number (OAN) exceeds 20 characters, enter the last 20 characters of the SER or OAN in the appropriate field and enter the complete number in the MIS field.

Effective July 2007, Credit Cards that are Lost, Found, Under Observation, Evidence, and Stolen are entered in the APS. Previously, only stolen credit cards could be entered. Items or merchandise purchased with a stolen credit card or credit card number are treated as “stolen” and should be entered into the APS. Remember, credit card records are not forwarded to NCIC. Also, the APS does not accept “securities”. Enter securities in the NCIC Security File. When multiple items of property are

reported stolen, lost, or are under observation in the same theft, crime report, or field interrogation card, they may be associated with one another by using the cross reference field (XRF).

The APS tables are updated on a daily basis and are available for download on the CLEW Web site at <http://clew.doj.ca.gov>.

K. AUTOMATED FIREARM SYSTEM (AFS)

Law Enforcement Record Types must be retained indefinitely (except Crime Gun and Evidence records which are retained for 10 years), or until the firearms are recovered/found/no longer under observation/ etc., until canceled, or determined to have been entered in error. Most Historical Firearm Record Types are also retained indefinitely (refer to the CJIS AFS manual). A firearm reported to the DOJ by the owner as no longer being owned by that person is entered as a No Longer Owned record. The associated No Longer in Possession (NLIP) form is available on the Attorney General's website at: www.ag.ca.gov/firearms/forms. Firearms that have been used in a crime, suspected of being used in a crime, illegally possessed, have obliterated serial numbers, or associated with a suicide or attempted suicide, shall be reported to the DOJ as Crime Guns and shall be entered as soon as possible.

Stolen and Found firearms records may be entered into AFS only (ENT/1), or they may be entered into both the AFS and NCIC Gun Files (ENT/2). Effective April 4, 2008, changes were made to AFS to also allow Lost records to be entered simultaneously in AFS and NCIC using ENT/2. Lost records currently in the AFS will remain as CA only records. If the entering agency wishes a Lost record to be entered into AFS and NCIC, it must cancel the original entry and re-enter the record as ENT/2. (*DOJ Information Bulletin 2008-BOF 04*)

NATIONAL CRIME INFORMATION CENTER NCIC

L. IDENTITY THEFT FILE (ITF)

The ITF serves as a means for law enforcement to flag stolen identities and identify the imposter when encountered by law enforcement. Information entered into the ITF will create a 'victim profile' that is made readily available to law enforcement during future encounters, such as routine traffic stops. Documentation for the entry of an identity theft record must meet the following criteria: 1) someone other than the victim is using the identification, 2) the identity is being used without permission, and 3) the victim's identity is being used or is intended to be used to commit an unlawful activity. Enter NCIC Identity Theft records directly into NCIC.

M. SECURITIES FILE

The Securities File contains records for securities that were stolen, embezzled, used for ransom, or counterfeited. Securities are identified as currency and documents or certificates that are evidence of debt or ownership of property or documents that represent subscription rights. Items which do not meet the definition for entry in any NCIC 2000 file are personal notes; bank drafts; cashier's checks; bank officer's checks; certified checks; personal checks; company checks; U.S. Treasury checks, and other types of government checks (state and local); lost or stolen credit cards; gold and silver coins; gift certificates; and savings and checking account passbooks. Serialized food coupons (stamps and books), ingots, lottery tickets, and medals do not qualify as securities for NCIC purposes, but may be entered in the NCIC Article File. California does not have a corollary Securities File. Enter Securities directly into NCIC.

N. VIOLENT GANG TERRORIST ORGANIZATION FILE (VGTOF)

The VGTOF is composed of two components or “capabilities,” both intended to accomplish the two major goals of the file: 1) promoting the identification of groups and group members, and 2) facilitating the exchange of information about these groups and members. The Group Reference Capability (GRC) provides information about gangs and terrorist organizations. This capability can be accessed by an individual QGG inquiry. The Group Member Capability (GMC) provides information in a format similar to Wanted Person File records about individual members of gangs or terrorist organizations. This capability can be accessed by an individual QGM inquiry and by automatic cross-search with all files searched by a Wanted Persons inquiry (or any related transaction, such as an entry which generates an inquiry).

The first agency (primary ORI) which enters a particular group/subgroup combination for a gang or terrorist organization GRC record is responsible for all fields of the base record and supplemental record except for additional ORI/Point of Contact (POC) data entered by subsequent originating agencies. Subsequent entries for that particular group/subgroup will be permitted to allow another agency to express an interest by adding its own ORI and point of contact information. The subsequent agency cannot enter or modify any field in the record other than its own ORI or POC Fields. If subsequent entries contain data in the restricted Fields, that data will be ignored. Any agency with pertinent additional information should contact the primary ORI/POC to request a modification of the GRC record information, when appropriate.

SECTION TWO

FULL ACCESS OPERATOR WORKBOOK QUESTIONS

Name: _____

Date: _____

Score: _____

(70% Passing Score Acceptable)

GENERAL POLICIES AND LIABILITY/SECURITY ISSUES

46. It is required that each employee/volunteer sign an employee statement form prior to operating or having access to CLETS terminals, equipment or information. This form addresses:
- A. Confidentiality
 - B. Penalties for the improper release of criminal history
 - C. Misuse of CLETS information
 - D. All of the above

RECORD MAINTENANCE RESPONSIBILITIES

47. All entries must be double-checked by a second party at the time of entry.
- A. True
 - B. False
48. An agency receiving a hit confirmation request must respond with a substantive response. A substantive response is defined as:
- A. Hit confirmed
 - B. Hit denied
 - C. Unable to respond at this time. Will reply in (specify time)
 - D. All of the above

CRIMINAL JUSTICE INFORMATION SYSTEM (CJIS)

WANTED PERSONS SYSTEM (WPS)

49. What may be entered into the WPS to indicate special handling of a person or to relay vital information for officer safety?
- A. Warning codes
 - B. Caution and Medical Condition codes
 - C. Miscellaneous codes
 - D. Public Safety Codes

50. A locate transaction can only be used when your agency has apprehended the subject of a wanted person record entered by your agency.
- A. True
 - B. False

CALIFORNIA RESTRAINING AND PROTECTIVE ORDER SYSTEM (CARPOS)

51. Should a mandatory Restraining Order be entered into the CARPOS even though the order has not been served on the subject?
- A. Yes
 - B. No
52. Records residing in the 30 day suspense file can be re-activated by modifying which field(s)?
- A. File control number
 - B. Restrained person name
 - C. Expiration date
 - D. All of the above
53. Records in the history file will be purged from the CARPOS history file after how long?
- A. On the 31st day after expiration or cancellation date
 - B. 5 years from the initial date of entry
 - C. 5 years, 30 days from expiration or cancellation date
54. Records in suspense can only be accessed by the originating agency.
- A. True
 - B. False

SUPERVISED RELEASE FILE (SRF)

55. Local law enforcement agencies may enter subjects into which of the SRF indices?
- A. Career Criminal
 - B. Probation
 - C. Department of Mental Health
 - D. All the above
56. When is it acceptable to enter a record into the SRF production database for training and testing purposes?
- A. When giving required CLETS training to staff
 - B. Using John Doe as the test name
 - C. Never - use the SRF test/training message keys

MISSING AND UNIDENTIFIED PERSONS (MUPS)

57. According to federal statute, missing persons under the age of _____ are required to be entered into state and national missing person files immediately.
- A. 12
 - B. 16
 - C. 18
 - D. 21
58. Photographs and dental X-rays of missing persons should be sent to the MUPS Unit on all open cases.
- A. True
 - B. False
59. Suspect and vehicle information should be entered in separate supplemental transactions, and not solely in the MIS field of a missing person base record.
- A. True
 - B. False

SEX AND ARSON REGISTRATION (SAR) – VIOLENT CRIME INFORMATION NETWORK (VCIN)

60. If an individual has registered with one agency, and then subsequently moves to another agency's jurisdiction, should the new agency create an additional sex registration record?
- A. Yes
 - B. No
61. What agency can cancel or clear an SAR record?
- A. Any agency contributing information to the SAR record
 - B. The DOJ SOTP Unit at 916-227-3288
 - C. Both of the above

STOLEN VEHICLE SYSTEM (SVS)

62. In Stored and Impounded vehicle records, which data field should be used to enter the place of vehicle storage and telephone contact information?
- A. Miscellaneous field
 - B. Reference field
 - C. Both of the above
 - D. None of the above

63. The entry of a stolen vehicle record into the SVS is not required if the vehicle is recovered before the entry is made.
- A. True
 - B. False

AUTOMATED BOAT SYSTEM (ABS)

64. Why should repossessed and stored vessels be entered into the ABS?
- A. To avoid the later entry of erroneous stolen boat records
 - B. To avoid a fine by the DMV

AUTOMATED PROPERTY SYSTEM (APS)

65. Are agencies required to enter non-serialized property into the APS that has been uniquely inscribed?
- A. Yes
 - B. No
66. Unique inscription data should be entered in what field to make it searchable?
- A. OAN
 - B. SER
 - C. MISC

AUTOMATED FIREARMS SYSTEM (AFS)

67. How long is the retention period for firearm records entered as Safekeeping, Under Observation, Lost or Stolen, and Buy?
- A. 90 days
 - B. 6 months
 - C. One year
 - D. Indefinitely or until cancelled
68. Crime Gun records include records of:
- A. Firearms associated with suicides/attempted suicides
 - B. Firearms with obliterated serial numbers
 - C. Firearms used/suspected in a crime
 - D. Illegally possessed firearms
 - E. All the above

NATIONAL CRIME INFORMATION CENTER (NCIC)

IDENTITY THEFT FILE (ITF)

69. Documentation for the entry of an ITF record must meet which of the following criteria?
- A. Someone other than the victim is using the identification
 - B. The identity is being used without permission
 - C. The victim's identity is being used or is intended to be used to commit an unlawful activity
 - D. All of the above

SECURITIES FILE

70. The Securities File contains records for securities that were:
- A. Stolen
 - B. Embezzled
 - C. Used for ransom
 - D. Counterfeited
 - E. All of the above
 - F. None of the above

VIOLENT GANG AND TERRORIST ORGANIZATION FILE (VGTOF)

71. Modification or entry of additional information to a Group Reference Capability record, other than ORI/POC data, can only be done by the primary ORI.
- A. True
 - B. False