CALIFORNIA LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEM
SUBSCRIBER AGREEMENT

Print Form

Department of Justice
CLETS Administration Section
P.O. Box 903387
Sacramento, CA 94203-3870

Telephone (916) 227-3677
Fax (916) 227-0696

cas@doj.ca.gov

ORI# _____ County _____

In accordance with Section 15165 of the Government Code, it is hereby agreed that

_____
(Name of Agency or Organization)

hereinafter referred to as Subscriber, as a Subscriber to the California Law Enforcement Telecommunications System (CLETS), will conform to the operating policies and regulations of the California Department of Justice (CA DOJ) and the Federal Bureau of Investigation (FBI).

It is further agreed by the Subscriber that, to receive such criminal history information as is available in the FBI files and in the CA DOJ files, the Subscriber agrees to abide by all rules and policies of the FBI as approved by the National Crime Information Center (NCIC) Advisory Policy Board. The Subscriber also agrees to adhere to all rules and policies of the National Law Enforcement Telecommunications System. No private entity shall be authorized to access the CLETS, nor shall the CLETS be used on behalf of a private entity for purposes of parking citation enforcement.

It is understood by the Subscriber that violation of these policies and regulations may result in suspension of service or other appropriate disciplinary actions as determined by the CA DOJ, with recommendation from the CLETS Advisory Committee.

The CA DOJ reserves the right to immediately suspend furnishing criminal offender record information to the Subscriber when either security or dissemination requirements are violated.

It is understood by the Subscriber that it is the responsibility of all city, county, state, and federal agencies that use information from the CLETS to participate in the CA DOJ's training programs to ensure all personnel (i.e., terminal operators, peace officers, investigators, clerical, agency management/supervisors, etc.) are trained in the operation, policies, and regulations of each file that is accessed or updated. Subscriber understands that training shall be provided only by the CA DOJ's training staff or another certified CLETS/NCIC trainer. Periodic unannounced site inspections may be performed by the CA DOJ to ensure compliance with the criminal offender record information regulations and CA DOJ policies.

CALIFORNIA LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEM SUBSCRIBER AGREEMENT

ORI# _____ County _____

It is further agreed by the Subscriber that the following training requirements will be followed:

1. Initially (within six months of employment or assignment) train, functionally test, and affirm the proficiency of all terminal (equipment) operators (full access/less than full access) by the completion of a Proficiency Examination (or facsimile thereof) to ensure compliance with the CLETS/NCIC policies and regulations.

2. Biennially provide functional re-testing and reaffirm the proficiency of all terminal (equipment) operators (full access/less than full access) by the completion of a Proficiency Examination (or facsimile thereof) to ensure compliance with the CLETS/ NCIC policies and regulations.

3. Maintain record of all training, testing, and proficiency affirmation. An individual computerized or written log must be maintained on each full access operator. Such logs may be destroyed three years after the operator is separated from the agency. Training records for less than full access operators, practitioners, administrators, and other sworn/non-sworn law enforcement personnel shall be maintained on a computerized or written group log. Less than full access operator group access logs shall be retained indefinitely by the agency. The examinations may be discarded upon entry of the required information in the appropriate log.

4. Initially (within six months of employment or assignment) all sworn law enforcement personnel must receive basic training in the CLETS/NCIC policy and regulations.

5. Make available appropriate training on the CLETS/NCIC system use for criminal justice practitioners other than sworn personnel.

6. All sworn law enforcement personnel and other practitioners should be provided with continuing access to information concerning the CLETS/NCIC systems, using methods such as roll call and in-service training.

7. Provide peer-level training on the CLETS/NCIC system use, regulations, policies, audits, sanctions, and related civil liability for criminal justice administrators and upper-level managers.

Either the CA DOJ or the Subscriber may, upon 30 days notice in writing, discontinue service. This Subscriber Agreement shall be renewed when the agency head changes or immediately upon request of the CA DOJ.

_____ _____
Agency Head Name Title

_____ _____
Agency Head Signature Date

CLETS SECURITY POINT OF CONTACT DELINEATION AND AGREEMENT

Print Form

A Security Point of Contact (SPOC) is the person designated to serve as the security coordinator with the California Department of Justice (CA DOJ) on security matters pertaining to the use of the California Law Enforcement Telecommunications System (CLETS), the National Crime Information Center (NCIC), the National Law Enforcement Telecommunication System (NLETS), CA DOJ criminal justice databases, and the administrative network the CLETS supports. If a consultant is to perform any of these duties, an agency representative must review and approve all proposed actions. The SPOC shall coordinate with the Agency CLETS Coordinator (ACC) on all routine or non-emergency actions or matters pertaining to the CLETS, the NCIC, the NLETS, CA DOJ criminal justice databases, and the administrative network that the CLETS supports. When feasible, the SPOC shall coordinate with the ACC on all exceptional or emergency actions in matters pertaining to the CLETS, the NCIC, the NLETS, CA DOJ criminal justice databases, and the administrative network the CLETS supports.

Requirements

- Be familiar with all security aspects of the agency's CLETS, CA DOJ criminal justice databases, NCIC, and NLETS connected devices and infrastructure.
- Possess a strong technical foundation and be able to coordinate and perform security-related activities as required.
- Be authorized and have access to all technical components and documentation related to the agency's segment of the CLETS infrastructure.
- Ensure emergency critical changes or modifications, etc., to the agency's CLETS infrastructure, as directed by the CA DOJ, are performed with little or no advanced notice.
- Have access to security and system audit logs that either directly or indirectly support CLETS infrastructure. This shall not include access to the CLETS journal information or data.

Roles and Responsibilities

Administration

- Coordinate with the ACC to establish procedures ensuring only authorized users have access to the CLETS and its related hardware or software.
- Coordinate or respond to the CA DOJ security-related correspondence.
- Ensure that a backup SPOC is designated. If the primary SPOC cannot be located or contacted, the backup SPOC shall assume all SPOC responsibilities.
- Retain all documentation and notify the agency head if the individual no longer serves as the SPOC.

Audits/Inspections/Validations

- Coordinate with the ACC to ensure the continued availability, confidentiality, and integrity of the CLETS infrastructure residing in the agency's systems or networks.
- Coordinate with the ACC to recommend proactive or corrective actions necessary to validate or verify the agency's compliance with the CLETS Policies, Practices, and Procedures (PPP).
- Coordinate with the ACC to recommend actions necessary to ensure compliance with all state or federal auditing requirements as described in the CLETS PPP.
- Coordinate the agency's CLETS security inspections by the CA DOJ network information security or field liaison staff, as required or requested by the CA DOJ.

CLETS SECURITY POINT OF CONTACT DELINEATION AND AGREEMENT

Policy

- Recommend to the ACC actions necessary to ensure compliance with all applicable CA DOJ, CLETS, NCIC, or NLETS security practices, policies, statutes, or regulations.
- Recommend to the ACC the actions necessary to ensure the CLETS terminals, equipment, or messages are secure from unauthorized access.
- Recommend to the Agency Head the actions necessary to establish a security incident response for the agency to discover, investigate, document, or report incidents that endanger the security or integrity of the CA DOJ systems or networks.
- Recommend to the Agency Head a security incident response (defined above), reporting procedures.

System

- Have a current system diagram available.
- Have a list of all the CLETS terminal locations within the agency available, identifying the terminal as fixed, mobile, behind a Local Area Network, Wide Area Network, etc.
- Have a list of all the CLETS terminal mnemonics (static or pooled) available.
- Review the CLETS applications for new, upgraded, or changing services for compliance with security requirements.
- Retain or have access to all records of changes or problems associated with CLETS hardware or software.

Training

- Coordinate with the ACC to ensure security awareness training is provided to all agency CLETS users within the first six months of employment or appointment and every two years thereafter.

Signatures indicate you have read, understand, and pledge to abide by this SPOC delineation and agreement.

SPOC Acknowledgement:

Printed Name _____ Date _____

Signature _____

Agency Head SPOC Acknowledgement Confirmation:

Printed Name _____ Date _____

Signature _____

THIS ORIGINAL AGREEMENT SHALL BE MAINTAINED BY THE AGENCY

ORI Number CA009013G

County El Dorado

CALIFORNIA SEX AND ARSON REGISTRY (CSAR)
Agency User Agreement

County of El Dorado-Probation Department

(Name of Agency)

Hereinafter referred to as the Subscriber, your agency agrees to conform to all rules and policies established by the Department of Justice (DOJ) in the *Security, Policies, Practices and Procedures* for the CSAR Web Interface. CSAR information and images are confidential and are to be used for law enforcement purposes only. Use of the CSAR for any other purpose may be a violation of California Penal Code sections 290 and 457.1. It is understood by the Subscriber that violation of these rules, policies, practices and procedures may result in suspension or revocation of CSAR access, as deemed appropriate by the DOJ. In signing this Agency Agreement, the Subscriber is certifying that he/she is a regularly employed peace officer or other law enforcement representative.

It is understood by the Subscriber that it is the responsibility of all agencies using the CSAR to participate in the DOJ's CSAR training. All personnel (i.e., computer operators, peace officers, investigators, clerical, agency management/supervisors, etc.) must be trained in the operation, policies, and procedures of the CSAR. The Subscriber understands that training can only be provided by DOJ's training staff, the local agency's CSAR Justice Identity Manager System (JIMS) Administrator, or the agency's CSAR Trainer.

The DOJ, and/or the Agency's CSAR-JIMS Administrator will perform audits on the use of the system and its records to ensure compliance with the CSAR *Security, Policies, Practices and Procedures* and to validate the timeliness, accuracy, and completeness of the data. Periodic, unannounced site inspections may be performed by the DOJ to ensure compliance with the above.

Agency Executive Officer (Printed Name)

Title

Phone Number

Signature

Date

Please return the completed and signed agreement to the Department of Justice, California Sex and Arson Registration Implementation Program (CSAR IP) via e-mail VCIC.CSAR@doj.ca.gov or fax to (916) 227-4814.

SECURITY POLICIES, PRACTICES AND PROCEDURES
for the California Sex Arson Registry (CSAR) Web Interface

I. Purpose and System Description

Pursuant to California Penal Code (PC) Section 290.022, the California Sex and Arson Registry (CSAR) is California's mandated repository for sex and arson registration information. Registering agencies, (i.e., local police and sheriff departments) are mandated to use the CSAR to register, track, and monitor their sex and arson registrants. Law enforcement and other criminal justice agencies also use the CSAR to obtain information on sex and/or arson registrants for investigations, tracking or monitoring, and prosecutorial purposes.

Agencies can access the CSAR via the following interfaces: the California Law Enforcement Telecommunication System (CLETS), the LiveScan Registration, Type-of-Transaction, and the Web Graphical User Interface (GUI). The security policies, practices and procedures detailed in this document only apply to the CSAR Web GUI interface. For the purposes of this document, "Law Enforcement" refers to both law enforcement and criminal justice agencies.

The CSAR application is maintained by the California Department of Justice (DOJ), CSAR Implementation Program (IP), and the Hawkins Data Center (HDC). The CSAR is accessed and utilized from a personal computer (PC) web browser in a secure network environment. The CSAR utilizes the secure DOJ communication network. Users of CSAR must have a secure connection to the DOJ network..

II. Eligibility for Access

Regularly employed peace officers or other law enforcement representatives are eligible to access the CSAR. CSAR information and images are confidential and are to be used for law enforcement purposes only. Use of the CSAR for any other purpose may be a violation of California PC sections 290 and 457.1. It is understood by the user that violation of these rules, policies, practices and procedures may result in suspension or revocation of CSAR access, as deemed appropriate by the DOJ, CSAR IP.

III. Request for Service

All agencies requesting access to the CSAR must send the DOJ a completed CSAR Agency User Agreement (Exhibit 1 in the CSAR Security Policies, Practices and Procedures) signed by the agency's Executive Office. A new CSAR Agency User Agreement shall be updated at least every five years or immediately upon request of the DOJ. A CSAR Agency User Agreement can be obtained from the DOJ by contacting the CSAR IP or downloaded from the California Law Enforcement Website (CLEW).

IV. Roles and Responsibilities

Each agency must designate an Administrator(s) who will act as a liaison with the DOJ and maintain responsibility for coordinating the necessary system setup and maintenance functions. This Administrator will utilize the Justice Identity Management System (JIMS) to add, modify, and deactivate CSAR user accounts. The JIMS provides account management services for the CSAR and other DOJ applications.

The CSAR JIMS Administrator roles and responsibilities are:

- Serving as the primary point of contact between their agency and the CSAR IP;
- Disseminating information from the DOJ to their agency's CSAR users regarding the CSAR or other sex and arson registrant related information;
- Establishing and managing CSAR users accounts for their agency;
- Auditing the use of the CSAR by their users, and enforcing all CSAR security policies, practices and procedures;
- Ensuring the proper configuration of the agency network and/or personal computers to enable access to the DOJ Extranet. This responsibility will extend to network connectivity at remote offices under the jurisdiction of that agency. If the agency currently accesses the DOJ Extranet via a regional network maintained by another agency, it is not necessary to designate a Network Administrator.

V. User Agreements

All CSAR JIMS Administrators must complete a CSAR JIMS Administrator Agreement (Exhibit 2 in the CSAR Security Policies, Practices and Procedures). A CSAR JIMS Administrator Agreement can be obtained by contacting the CSAR IP or downloaded from the CLEW. The Agreement must be signed by the CSAR JIMS Administrator's immediate supervisor and sent to CSAR IP before access will be granted by to the CSAR IP.

All other users requesting access to the CSAR must complete a CSAR User Agreement (Exhibit 3 in the CSAR Security Policies, Practices and Procedures). Agreements can be obtained from the agency's CSAR JIMS Administrator, by contacting the CSAR IP, or downloaded from the CLEW. The CSAR User Agreement must be signed by the user's immediate supervisor before access will be granted by the agency's CSAR JIMS Administrator.

VI. Security/Audits

1. CSAR records are considered confidential and are to be used for law enforcement purposes only. All transactions are programmatically logged and subject to audit by the DOJ or the Federal Bureau of Investigation (FBI). Use of the CSAR for any other purpose may be a violation of California PC sections 290 and 457.1. It is understood by the user that violation of these rules, policies, practices and procedures may result in suspension or revocation of CSAR access, as deemed appropriate by the DOJ, CSAR IP.

2. All CSAR users must be fingerprinted and have a fingerprint check response on file *at their agency* prior to being granted access to CSAR. The minimum background requirements include a State Department of Justice fingerprint check (except (FBI offices) and an FBI fingerprint check.

3. Each employee having access to CSAR is required to sign the CSAR User Agreement prior to operating or having access to CSAR.

4. Agencies are required to have the CSAR User Agreement on file for each employee accessing the system.

5. CSAR terminals and information must remain secure from unauthorized access.

VII. CSAR Confidentiality Rules

1. Only authorized law enforcement or criminal justice personnel may access CSAR. Any information accessed via CSAR is confidential and for official use only by authorized law enforcement personnel. Access is defined as the ability to enter, view or print information via the CSAR.

2. Access to information through the CSAR is on a "right- to- know" and a "need- to-know basis".

3. Accessing and/or releasing CSAR information for non-law enforcement purposes is prohibited, and is subject to administrative action and/or criminal prosecution based on state or federal law.

4. CSAR terminals and information must remain secure from unauthorized access.

5. All CSAR information shall only be transmitted electronically using FIPS end-to-end approved encryption from the DOJ network to an authorized endpoint within the secure CSAR subscribing agency network. At no time shall CSAR data be transmitted unencrypted.

6. All CSAR information retained must be stored in a secure and confidential file.

7. When an agency determines CSAR information is no longer needed, the

information shall be destroyed in a manner so that the identity of the subject can no longer be reasonably ascertained, (e.g., shredding).

8. Information received from the CSAR must be maintained separately from non-law enforcement information.

9. Terminals must be away from public view with a log-on/log-off, password process in place.

CSAR information shall not be released to the media, unless disclosure is authorized pursuant to Penal Code sections 290.45 or 290.46.

VIII. Usernames and Passwords

CSAR username and passwords requirements are established and governed by the JIMS account management application. The JIMS requires a unique individual username and user selected password for each employee. At a minimum, an electronic verification of manually keyed unique username and password is required to access the CSAR.

The JIMS requires the following authentication:

1. Passwords are a minimum of eight (8) characters to a maximum of twenty (20) characters in length and are case sensitive.

2. Passwords may be a combination of alphabetic and/or numeric characters chosen by the owner of the Username, and should not be identifiable with the person using them, such as names or initials of the user, or a family member.

3. Each user's password shall be changed at least once every ninety (90) days.

4. After a password expires or has been changed, it shall not be used by the same person for at least four iterations.

Each CSAR subscribing agency shall ensure that the following password policies are enforced:

1. Passwords shall not be displayed in a readable manner or written down.

2. Passwords shall be kept confidential.

3. Passwords may be reset by the CSAR JIMS Administrator when required.

4. Reset of the end user's password will require verification of the individual's identity.

5. Any automatic programming of a username or password for log-on purposes is prohibited.

6. Username and/or password will not be stored by the user computer in the web browser form.

7. Users shall not share their username/passwords for accessing the CSAR.

8. User names and passwords must not be maintained in a manner accessible by others.

9. A user account shall be deactivated if the user is no longer required to perform the duties related to the approved business purpose, is no longer employed by the subscriber agency, or has been suspended from employment. Deactivation of account must occur with five business days.

The DOJ and/or the CSAR JIMS Administrator shall immediately deactivate a user account if the user:

1. Is suspected of, or conducts an unauthorized access, disclosure, or misuse of CSAR records.

2. Does not comply with a security requirement identified within the CSAR Security Policies Practices and Procedures.

The session log-on will be programmatically terminated by CSAR after thirty (30) minutes of inactivity. Termination shall not be transparent to the user.

IX Network Security Requirements

The DOJ is responsible to ensure all network connections and physical media used to facilitate remote access to the DOJ network meets the following minimum requirements:

1. Only authorized clients shall be able to initiate a connection to the DOJ through the remote access connection.

2. All communication to and from the DOJ CSAR system shall be actively monitored and logged to ensure that only authorized communications and sessions are permitted over the remote access connection.

3. All remote access connections over a public transport (e.g. Internet) shall require all communications to be encrypted using FIPS approved encryption algorithms and encryption modules and be of at least 128 bits in strength.

4. Systems shall be monitored with an Intrusion Prevention/ Intrusion Detection System.

5. All customer premises equipment deployed to provide access to the DOJ network

(routers, etc.) will be actively maintained and managed by the DOJ network staff.

X. Subscribing Agency Endpoint Security

The CSAR subscribing agency shall ensure that all endpoints (workstations, laptops, etc.) that are used to access CSAR meet the following security requirements:

1. Have a subscription-based antivirus product/solution with current virus signatures loaded, and configured to protect the system in real-time. The anti-virus product /solution shall actively clean, quarantine, and/or remove any content and processes deemed to be unauthorized and/or malicious in nature. Anti-virus scanning of the disks shall be performed at least daily.

2. Have an anti-spyware product/solution with current spyware signatures loaded, and configured to protect the system in real-time. The spyware product/solution shall actively remove spyware from the system when it is detected. Spyware scanning of the disks shall be performed at least daily.

3. Use a manufacturer-supported Operating System (OS). The OS shall be kept up to date with all relevant critical patches and updates within two weeks of release from the manufacturer.

4. Be configured with a session timeout setting of 30 minutes of inactivity or less, prompting for re-login.

5. Not contain any software or utilities that allow for discovery, reconnaissance, fingerprinting or vulnerability scanning/penetration testing of the DOJ Network.

6. Require successful authentication to the CSAR system. All communications to DOJ systems shall be authenticated and not utilize anonymous, null, or guest accounts.

7. Be configured to log all successful and failed login and access attempts. These logs shall be protected from tampering and be retained for a period of no less than 90 days.

8. Employ a personal firewall on all devices.

9. The agency shall develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes.

XI. Security Incident Reporting

The subscribing agency shall immediately notify the DOJ by telephone and e-mail when a security incident(s) (e.g., lost or stolen token, compromised data, etc.) is known. Subscribing

agency support staff is expected to respond and resolve systems security issues that would include but not be limited to malicious code, policy violations, unauthorized access, intrusion and misuse of the systems and/or data. The subscribing agency shall send formal documentation within five (5) business days after the detection of the incident(s) detailing the incident and corrective actions taken to date.

CAL DOJ Security Incident Reporting contacts:
Network Information Security Section (NISS)
Stephanie Cervantes (916) 227-3105
NISU@doj.ca.gov
With a cc to the CAL DOJ Information Security Officer: DOJISO@doj.ca.gov

Technical staff must immediately notify their designated counterparts by telephone and e-mail when a security incident(s) is detected, so the other party may take steps to determine whether its system has been compromised and, take appropriate security precautions. The system owner will receive formal notification in writing within five (5) business days after detection of the incident(s).

XII. Training

DOJ will provide training and/or training materials to the CSAR JIMS Administrator. It will be the responsibility of these administrators to provide training to the users in their agency.

Quick Reference Guides, videos and other training material are available upon request to the CSAR IP and on the CLEW website at http://clew.doj.ca.gov. The CSAR User Guide is available on the CSAR application by clicking on the "Help" button.

XIII. California DOJ Contact Information

CSAR IP
4949 Broadway, Room B 216
Sacramento, CA 95820
(916) 227-4123
FAX (916) 227- 4814
e-mail: csar@doj.ca.gov

CALIFORNIA SEX AND ARSON REGISTRY (CSAR)
JUSTICE IDENTITY MANAGEMENT SYSTEM (JIMS)
ADMINISTRATOR AGREEMENT

Please complete and sign this agreement and return it to the California Sex and Arson Registry Implementation Program (CSAR IP). All fields are mandatory. This information will be used to authorize your access to the CSAR, and establish you as the CSAR-JIMS administrator for your agency. As the Administrator, you will serve as the point of contact between your agency and the CSAR IP. An agency may choose to have one or more administrators.

Upon completion, return the signed agreement to the CSAR IP via e-mail at VCIC.CSAR@doj.ca.gov or fax to (916) 227-4814. You will be assigned and advised of a default password, which you will be required to change when first accessing CSAR.

ADMINISTRATOR'S INFORMATION

First Name

Last Name

Title

Agency Name

Division/Unit

Address

City State

Zip Code Phone Number

E-mail Address

ORI Number

As the Administrator for your agency will you also be entering or updating registrant data into CSAR?

☐ No ☐ Yes

Administrator's Signature _____ Date _____

Supervisor's Signature _____ Date _____

Supervisor (Printed Name) _____ Phone Number _____

I understand that only authorized law enforcement or criminal justice personnel may access the CSAR. Any information accessed via the CSAR is confidential and for official use only by authorized law enforcement personnel. Access is defined as the ability to enter, view or print information via the CSAR.

Roles and Responsibilities of the CSAR-JIMS Administrator

Each agency must designate an Administrator(s) who will act as a liaison with the DOJ and maintain responsibility for coordinating the necessary system setup and maintenance functions. This Administrator will utilize the Justice Identity Management System (JIMS) to add, modify, and deactivate CSAR user accounts. The JIMS provides account management services for the CSAR and other DOJ applications.

The CSAR JIMS Administrator roles and responsibilities are:

- Serving as the primary point of contact between their agency and the CSAR IP.
- Disseminating information from the DOJ to their agency's CSAR users regarding the CSAR or other sex and arson registrant related information.
- Establishing and managing CSAR users accounts for their agency.
- Ensuring that the CSAR User Agreements are maintained, and that the Security Policies, Practices and Procedures for the CSAR web interface are distributed to each new user.
- Auditing the use of the CSAR by their users, and enforcing all CSAR security policies, practices and procedures.
- Ensuring the proper configuration of the agency network and/or personal computers to enable access to the DOJ Intranet. This responsibility will extend to network connectivity at remote offices under the jurisdiction of that agency. If the agency currently accesses the DOJ Intranet via a regional network maintained by another agency, it is not necessary to designate a Network Administrator.

State of California
Department of Justice
California Sex and Arson Registration Implementation Program
4949 Broadway, Room B-216
Sacramento, CA 95820
(916) 227-4123