USE OF THE CALIFORNIA SEX AND ARSON REGISTRY (CSAR) AND MEGAN'S LAW INFORMATION SYSTEM FOR COMMUNITY NOTIFICATION

AUTHORITY: Administrative Directive

RESCINDS: Procedure Manual Item 1-1-102, dated 04/18/14 (Recertified)

FORMS:

Megan's Law Disclaimer	(Attachment)
California Sex and Arson Registry (CSAR) User Agreement	(Attachment)
Security Policies, Practices and Procedures for the California Sex Arson Registry	(Attachment)

PURPOSE: To provide guidelines for use of the California Sex and Arson Registry (CSAR) and the Megan's Law Information System for community notification and education.

I. GENERAL INFORMATION

A. The Orange County Probation Department Sex Crimes Unit has been called upon to participate in community safety and education presentations, which have included public notification of registered sex offenders using the Megan's Law Information System. This information is available to the public and can be accessed at www.meganslaw.ca.gov. It posts sex offenders displayed by city, ZIP Code, county or within a predetermined radius of a selected address, park, or school. The Department of Justice (DOJ) posted the website in December 2004 (Section 290.46 PC and AB 488 chaptered 09/24/04). In December 2005, DOJ posted a privately accessed Megan's Law Intranet website for law enforcement agencies, which contained information on all registrants, including "no post" categories. In July 2010, DOJ created the California Sex and Arson Registry (CSAR) pursuant to Penal Code 290.022. The Orange County Probation deactivated access to the Megan's Law Intranet website for law enforcement agencies and activated access to the CSAR. Guidelines have been established to provide this information to the public in order to promote the Probation Department's mission of enhancing community safety.

B. The Orange County Probation Department authorizes staff, to access CSAR in compliance with the policies of the Probation Department and the Department of Justice. The Megan's Law Information System is available to the public and the Orange County Probation Department via the Internet.

C. The Division Director of the Special Supervision Division or designee (supervisor of the Sex Crimes Unit), acts as the Probation Department's CSAR administrator, hereinafter referred to as the "CSAR JIMS Administrator" (California Sex and Arson Registry Justice Identity Management System) and liaison to the California Department of Justice.

II. PROCEDURE

A. Access will be attained through the Internet, and/or the Probation Department Intranet (Prob-Net).

1. All Probation personnel authorized to access the CSAR will be designated by the CSAR JIMS Administrator or designee.

2. Authorized staff must sign the CSAR User Agreement (Attachment B) in acknowledgement of the Security Policies, Practices and Procedures for the CSAR Web Interface (Attachment C) under the direction of the CSAR JIMS Administrator prior to accessing the system.

3. Access to the CSAR has been granted to the Division Director of Special Supervision, as well as the supervisor and deputies of the Sex Crimes Unit. The CSAR JIMS Administrator or designee may also grant access to additional Probation Department staff as needed.

B. PUBLIC VERSION ACCESS

1. Public version access includes, but is not limited to, making limited information available to the public at county fairs, community notifications, town hall meetings, or individual requests from private citizens. Authorized Probation staff may access the public version in the case of such events, in compliance with the guidelines set forth by the Probation Department and Department of Justice.

2. The CSAR JIMS Administrator or designee is responsible for informing and receiving approval from Executive Management prior to any public display of the Megan's Law Information System.

3. Prior to viewing the public version, citizens must acknowledge they have read the Megan's Law Disclaimer and agree to its Terms and Conditions (Attachment A).

4. Individual requests to view the public version may also be made directly to an authorized deputy. The above-stated procedure will apply.

5. Expedite all positive identifications, ("hits"), to the Sex Crimes Unit supervisor for further investigation.

C. CSAR ACCESS

1. CSAR provides deputies secure access to expanded information to assist with the registration, investigation, apprehension and supervision of registered sex offenders. The information available on CSAR provides complete sex registration records, risk assessment information, method of operation information, employment and vehicle information, sexually violent predator status and an ability to view registrant photos. CSAR is "read only" access. Authorized deputized staff may also access the database to supplement investigations by other law enforcement agencies, or to protect the public regardless of whether or not the offender is on probation.

2. Deputized staff may also request to view CSAR by contacting any deputy or unit supervisor assigned to the Sex Crimes Unit and acknowledge penalties for misuse of sex offender registrant information.

REFERENCES:

Procedures:	1-1-101	Access to and Release of Criminal Offender Record Information (CORI)
	1-1-107	Release of Sex Offender Information to the Public
	1-4-114	Reporting Unusual or Special Incidents
	2-1-004	Child Abuse Reporting Responsibilities of Deputized Probation Staff
	2-1-005	Elderly Abuse and Dependent Adult Abuse Reporting Responsibilities of the Probation Officer
Policies:	A-1	Policy, Procedure and the Law
	A-2	Upholding Departmental Philosophy and Principles
	A-10	Contact with News Media
	A-17	Conflict of Interest
	A-21	Liability
	B-1	Case Confidentiality-Client's Right to Privacy
	B-2	Inter- and Intra-Agency Confidentiality
	B-3	Case File Management and Security
	B-4	Sensitive Cases
	E-8	Volunteers

Attachments

D. Haner

APPROVED BY: Digitally signed by Shawn E. Small
Date: 2016.06.27 11:15:39 -07'00'

Megan's Law Disclaimer

Read and acknowledge the disclaimer at the bottom of page.

Informational Only. The California Department of Justice has not considered or assessed the specific risk that any convicted sex offender displayed on this web site will commit another offense or the nature of any future crimes that may be committed.

Legal Limits on Disclosures. Only information on registered sex offenders allowed to be disclosed under California law appears on this web site. Under state law, some registered sex offenders are not subject to public disclosure, so they are not included on this site. State law does not allow offenses other than the crimes for which the convicted sex offender is required to register to be disclosed here.

Errors and Omissions. Information pertaining to schools, parks and street map data is obtained with permission of and through a license agreement with TomTom. Other information on this web site is compiled from reports by local law enforcement. Much of that information is gathered from persons who are required to register as sex offenders and to provide, at least once a year, their addresses and other information to local law enforcement. Because information can change quickly, and there may be gaps in data received, the California Department of Justice makes no representation, either express or implied, that the information on this site is complete or accurate. Neither the Department of Justice nor the State of California shall be held responsible for any errors or omissions on this web site or produced by secondary dissemination of this information.

Mistaken Identities. Extreme care must be taken in the use of information because mistaken identification may occur when relying solely upon name, age and address to identify individuals.

Notice of Corrections. If you believe that any information on this site is in error, please contact a police or sheriff's department, or contact the Department of Justice by e-mail at MegansLaw@doj.ca.gov.

Legal and Illegal Uses. The information on this web site is made available solely to protect the public. Anyone who uses this information to commit a crime or to harass an offender or his or her family is subject to criminal prosecution and civil liability. Any person who is required to register pursuant to Penal Code section 290 who enters this web site is punishable by a fine not exceeding $1,000, imprisonment in a county jail not exceeding six months, or by both the fine and imprisonment. (Pen. Code, § 290.46, subd. (k).)

☐ I have read the disclaimer and agree to these terms and conditions. Continue

1-1-102
Attachment B

CALIFORNIA SEX AND ARSON REGISTRY (CSAR)
USER AGREEMENT

Please complete each of the fields listed below and return this form to your agency's CSAR-JIMS Administrator. All fields are mandatory. This information will be used to authorize your access to the CSAR. Contact your CSAR-JIMS Administrator if you have any questions.

Your CSAR-JIMS Administrator will assign and advise you of a default password which you will be required to change when first accessing CSAR. Please ensure that you have read and understand the *Security Policies, Practices and Procedures for the CSAR Web Interface.*

USER'S INFORMATION

First Name			
Last Name			
Title			
Agency Name			
Division/Unit			
Address			
City		State	
Zip Code		Phone Number	
ORI Number			

New User'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 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 CSAR.

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.

Developed 02/11/2013

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