PAROLELEADS2.0

AGENCY PARTICIPATION AGREEMENT

The California Department of Corrections and Rehabilitation (CDCR), Division of Adult Parole Operations (DAPO) has implemented Parole LEADS (Parole Law Enforcement Automated Data System) which provides parolee information to local law enforcement agencies over a secure internet connection. The DAPO Offender Information that will be provided to your agency using Parole LEADS is Criminal Offender Record Information (CORI). Releasing or copying CORI to non-authorized persons is a misdemeanor pursuant to Penal Code Sections 13302-13304. Providing any state summary criminal information or CORI to any person or system not authorized to receive it under Penal Code section 11105 et seq is not permitted and the person who provided it is guilty of a misdemeanor pursuant to Penal Code section 11142. Any violation of the afore-mentioned statutes may be referred to either the State Department of Justice (DOJ) or local entities forprosecution. CDCR expects the participating agency to ensure that no such violation occurs.

The CORI and state summary criminal information furnished by DAPO is for official law enforcement purposes only. Your department or agency is required to comply with all security and technical provisions of this agreement. Agency staff accessing information from Parole LEADS must have both a need to know and a right to know. Failure to abide by the terms of this agreement, including the attached Parole LEADS Policy and Procedures, may result in the termination of the sharing of Parole LEADS information with your department or agency.

DAPO makes no guarantee regarding the accuracy of Parole LEADS information, and strongly encourages all participating agencies to verify information with the local Parole Agent before taking any action or making any decision based on this information. Additionally, it is strongly recommended that a Parole Agent be involved, at least telephonically, in any parolee-related search.

The data provided by Parole LEADS is intended for crime analysis or other law enforcement uses only. Summary or statistical information and reports regarding DAPO offenders will not be released outside the law enforcement community (including the news media) without confirmation from DAPO's Director or designee that the data is accurate and complete. This paragraph is not meant to dissuade any agency from sharing Parole LEADS information with other law enforcement agencies as long as each disclosure is journaled according to CORI regulations. Such sharing will be on a need to know, right to know basis and will not involve the electronic exportation of multiple Parole LEADS records.

Parole LEADS CORI will be accessed exclusively from authorized computer workstations at the local law enforcement agency's place of business, including a temporary command center and field devices issued by the agency and complying with CORI regulations. Any other access, including access from any personally owned, remote, mobile or home-based computer, is prohibited.

User account maintenance will be the responsibility of authorized agency staff unless other arrangements are jointly agreed to by the agency and DAPO.

The attached Policy and Procedures and the attached Participating Agency Hold Harmless Agreement are a part of this agreement. The Policy and Procedures shall be adhered to by every user of Parole LEADS. DOJ and the DAPO Security Administrator or designee is authorized to audit agency security logs and security procedures at each individual worksite upon written notice.

I certify that I am the chief law enforcement official of my agency, and have the full power and authority to execute this agreement with CDCR. I will ensure that my employees, who access, copy, use CORI information or maintain user accounts in Parole LEADS will be advised of the contents of this agreement, the attached policy and procedures, and will complete DAPO approved training before using Parole LEADS data or performing account maintenance. I have signed the Parole LEADS Participating Agency Hold Harmless Agreement. I also understand that I must designate a "primary contact" person (see below) and must resubmit this request when I wish the "primary contact" designation changed. This primary contact person has the authority to speak for my agency as it pertains to Parole LEADS matters.

	Sheriff-Coroner	
Signature of Law Enforcement Agency's Chief Official	Title	Date Signed

John	McMahon	
First Name (Print or Type)	Last Name (Print or Type)	Agency Email

San Bernardino County Sheriff-Coroner	CA0360000
Agency Name	CLETS Agency ID (ORI#)

Primary Contact Name (Print or Type)	Primary Contact Work Number	Primary Contact's Work Email

POLICY AND PROCEDURES

Parole LEADS Mission Statement

The Division of Adult Parole Operations (DAPO) of the California Department of Corrections & Rehabilitation (CDCR) has implemented a Parole Law Enforcement Automated Data System (Parole LEADS) application that provides Criminal Offender Record Information (CORI) to qualified local California law enforcement agencies over a secure public internet connection, primary for crime analysis activities.

References

The Parole LEADS policies and procedures were developed using the following reference documentation:

- Assembly Bill 3X (AB3X) effective January 1, 1995
- Criminal Offender Record Information (CORI) Legislation & Policy
- AB3X System Functional Specification
- California Department of Corrections and Rehabilitation Operations Manual (DOM)

Parole LEADS System Description Overview

The Parole LEADS application is designed to allow controlled and secure access of selected parolee information through the public internet. The system takes advantage of the latest Internet and security technology. This allows authorized law enforcement crime analysts, investigators or agents to obtain parolee information from an extract of the DAPO Statewide Parolee database in two ways. Authorized agency users can either access information on a search query basis or request a database download consisting of the agency's "group" of parolee records updated after a user-selected date. The Parole LEADS application is the responsibility of DAPO, the owners of this information. DAPO will maintain Parole LEADS, while requiring the observance of the policies and procedures necessary to protect CDCR's data and information systems. The *Parole* LEADS application is designed to serve local crime analysis needs and tactical or street-level employment by investigators on departmental-issued portable devices such as laptops or smartphones.

The data provided by Parole LEADS is intended for law enforcement uses only. Summary or statistical information and reports regarding DAPO offenders will not be released outside the law enforcement community (including the news media) without confirmation from DAPO's Director or designee that the data is accurate and complete. This paragraph is not meant to dissuade any agency from sharing Parole LEADS information with other law enforcement agencies as long as each disclosure is recorded according to CORI regulations. Such sharing will be on a need to know, right to know basis and will not involve the electronic exportation of multiple Parole LEADS records.

The Parole LEADS application performs two primary functions:

1. Parolee Database Download (defined group only)
2. Search for Parolee Information (group or statewide)

Parole LEADS Database Extraction

The Parole LEADS Database Extraction uses information generated from the DAPO's Statewide Parolee Database. Using the internet to connect to the Parole LEADS Web Server, the download user requests a database download consisting of its group of records updated since a user-selected date. The request is sent through the Parole LEADS Web Server. The download request is handled in a background process. Downloaded parolee information is encrypted between the Parole LEADS Web Server and the agency.

Search for Parolee Information

An authorized agency is not limited in the number of Parole LEADS "search query" users. A Parole LEADS end user must have an internet connection utilizing one of the following web browsers:

- Mozilla Firefox Version 3.5 or later
- Microsoft's Internet Explorer Version 7 or later

The end user generates a search query to obtain specific information on parolees. The search query is processed by the Parole LEADS Web Server to retrieve relevant DAPO parolee database records. The results of this query are then displayed to the user. Request and response transactions are encrypted between the Parole LEADS end user and the WebServer.

Parole LEADS Information Security Policy

CDCR Department Operations Manual, Section 49020.1 (05/20/2013) states "*It is the policy of the California Department of Corrections and Rehabilitation (CDCR) to protect against the unauthorized modification, deletion, or disclosure of information included in agency files and databases. The Department regards its information assets, including data processing capabilities and automated files, to be essential resources. The Department shall assume full responsibility for ensuring the security and integrity of its information resources.*"

CDCR regards its information assets, including data processing capabilities and automated files, to be essential public resources. Many aspects of CDCR's operation would effectively cease in the absence of critical computer systems, including automated systems necessary for the protection of the public, staff and offenders in the custody or control of CDCR.

Accordingly, the agency must assume full responsibility for the proper use and protection of Parole LEADS information in its possession.

Parole LEADS Information Ownership and Custodial Responsibility

The CORI available on Parole LEADS is owned by the DAPO. Once a Parole LEADS database download or query is accomplished, the agency assumes full custodial responsibility for this CORI, while DAPO maintains ownership. **The agency has no authority to share, reproduce, publish or disseminate Parole LEADS information outside its agency or to use this information for non-law enforcement purposes.** This is in no way intended to restrict the agency from providing this information to multiple sites within its agency.

As with any CORI, Parole LEADS information may not be publicly broadcast unless it is encrypted. Since the State Department of Justice (DOJ) has legal oversight for compliance with CORI statutes, users or custodians of Parole LEADS information must also comply with DOJ's published "CLETS Policies, Practices, and Procedures."

Note: The DOJ publication "CLET Policies, Practices and Procedures" is available via the internet at the following site: CLETS, Policies, Practices, and Procedures. This document is available for download in the PDF format that requires Adobe Acrobat Reader. The CLETS site above has a link to the site that makes the Adobe Acrobat Reader available for download.

Parole LEADS Security Concept of Operations

The Parole LEADS end users are required to use Mozilla (version 3.5 or later) or Microsoft's Internet Explorer (version 7.0 or later) browsers which applies the Secure Sockets Layer (SSL) with 128-bit encryption.

User identification and authentication is accomplished through the use of a reusable logon identifier and password at the Parole LEADS Web Server.

Security management provided by the Parole LEADS Security Administrator can be contacted at ParoleLEADS2@cdcr.ca.gov.

Parole LEADS Information Security Procedures

Agency Enrollment Process

In order to gain access to Parole LEADS, a local law enforcement agency must be physically located in California. Additionally, they must already access Criminal History Information from the California Law Enforcement Telecommunications System (CLETS) and be free of sanctions from either DOJ or CLETS Advisory Committee. The agency will be required to execute a Parole LEADS Agency Participation Agreement, which is provided as an attachment to this document and a Participating Hold Harmless Agreement. Both these agreements must be signed by the agency head, the highest level authority within the agency, usually the Chief of Police or the Sheriff. The Agency Participation Agreement emphasizes the importance of handling CORI properly, outlines the operational environment through which Parole LEADS may be accessed, and requires agency to follow the Parole LEADS Policies and Procedures. The Agency's chief official must also designate a "primary contact" for the agency. This person will have the authority to speak on behalf of the agency on Parole LEADS matters and approve all their agency's users and be the sole contact to deal directly with the Parole LEADS Security Administrator or designee. All requests for Parole LEADS access must be approved by, and routed through, this primary contact person. If the "primary contact" person is to be changed, a revised Agency Participation Agreement signed by the head of the agency is required. Once an agency is approved for Parole LEADS access, each end user will be required to complete a Parole LEADS End User Agreement. Law enforcement agencies interested in gaining access to the Parole LEADS application should direct e-mail to ParoleLEADS2@cdcr.ca.gov.

End User Site Requirements

The Parole LEADS end user physical sites are required to provide adequate controls and countermeasures to protect the CORI. Parole LEADS CORI shall be accessed exclusively from authorized computer workstations physically housed authorized agency's place of business or law enforcement-issued portable devices such as laptop or notebook computers and "smart" phones. **Any other access, including access from any personally owned, remote, mobile or home-based computer is expressly prohibited.**

All agencies' computer facilities with access to Parole LEADS are required to have physical controls to prevent unauthorized access due to the sensitivity of CDCR computer systems. Agency-issued portable devices such as laptop or notebook computers and "smart" phones must employ safeguards to prevent unauthorized access to Parole LEADS CORI information. Each custodian of Parole LEADS information shall establish physical and software controls over its information assets. It is required that someone be assigned to manage the end user system, including the security of the information it contains.

Parole LEADS Operations & Maintenance

System Startup

The first screen that any user sees after logging into Parole LEADS shall display the Terms and Conditions for using the application.

Parole LEADS System Updates/Changes

All Parole LEADS system updates or changes relating to CORI data security or end user access shall be approved by the Parole LEADS Information Security Office. Once approved, Enterprise Information Systems (EIS) shall implement and enforce those changes. Strict configuration management of Parole LEADS shall be enforced by EIS at all times.

Parole LEADS Database Extraction

The Parole LEADS Database Extraction uses information generated from the DAPO's Statewide Parolee Database. The time frame required for extracting information from the CDCR organizational network varies according to the date entered and the number of records returned for the particular agency unit code as defined earlier. Parole LEADS is the delivery mechanism for parole data contained within SOMS, an offender management system used exclusively by CDCR. Parole LEADS is updated with current parolee information every 20 minutes from SOMS to provide near real-time data to local law enforcement. **DAPO makes no guarantee regarding the accuracy of Parole LEADS information, and strongly encourages all participating agencies to verify information with a local Parole Agent before taking any action or making any decision based on this information.**

It is important that all users be adequately trained to use Parole LEADS but also to notify the Parole LEADS Security Administrator or designee regarding database inconsistencies or errors to ensure proper resolution.

With every database download there will be a separate index file of CDC numbers provided. This file contains a list of parolees who should be found in the parolee database after the download. When the agency's database is built from sequential database downloads (based on a user defined date) it is imperative that the agency, at the conclusion of each sequential download, compare this index file with the database to assure information integrity. If there are any discrepancies, the user may have to repeat the download based on different dates or request a new full download. Failure to apply this error correcting mechanism consistently may allow parolee information to become inaccurate and may constitute grounds for suspension or termination of Parole LEADS access.

Parole LEADS Logon and Password Standards

Access to Parole LEADS is restricted by a reusable password for authorized persons only. Authorized persons shall never reveal their passwords to anyone for any reason, nor record them or display them in a location or manner where others may discover them. Authorized persons engaging in a computer session shall log off before leaving the immediate vicinity of the terminal because the password that allowed the session to begin remains in effect throughout the session. Violation of this policy will result in the revocation of all user access privileges and appropriate disciplinary action. Such disciplinary action may be based not only on the violation itself, but also on all activity performed by those using the password.

As defined in the attached Agency Participation Agreement, the integrity of user accounts, such as ensuring the user is an active member of that agency, will be the responsibility of agency staff unless other arrangements are jointly agreed to by the agency and DAPO. A separate Account Password Administration Agreement for those assigned as Password or Account Administrators for their respective agency shall be submitted after the user reviews the training materials available in Learning Management Section (LMS) in Parole LEADS.

Whenever an authorized person terminates employment or is reassigned to duties that do not require access to Parole LEADS, the "primary contact" for the authorized agency shall, without delay, notify Parole LEADS Security Administrator or designee.

There is a need to ensure that authority to access Parole LEADS is restricted to persons with a demonstrated right and need for access. The request for each Parole LEADS account will first be approved by the agency's "primary contact" with this "need to know, right to know" concept in mind.

The lack of use of Parole LEADS is assumed to be evidence that the use is no longer required. Accounts may be disabled without notice if they are not used regularly.

Password Policy

Passwords shall be a minimum of eight (8) characters consisting of a least one upper case letter, one lower case letter and one number.

The Parole LEADS Security Administrator shall be responsible for ensuring each authorized user's password can be set, reset, and/or changed either through user initiated or System Administrator initiated.

Security questions within the account profile of an authorized user will be utilized to confirm identity before the password is reset. If a password is forgotten or compromised, the end user must immediately take action to change their password or contact the Parole LEADS Security Administrator or designee.

Parole LEADS end users shall be responsible for promptly notifying the Parole LEADS Security Administrator or designee a user ID and password should be disabled.

Each Parole LEADS end user shall be responsible for changing his or her password at least once every 75 days to counter the possibility of undetected password compromise.

A password shall be invalidated at the end of 90 days. A user who logs on with an ID having an expired password shall be required to change the password for that user ID before further access to the system is permitted.

Parole LEADS Security Audit Records Management

Parole LEADS generates security audit records at each of the firewalls, as well as at the various servers. The Parole LEADS Information Security Office (ISO) shall ensure that security audit records be reviewed to detect potential attacks on Parole LEADS, and that appropriate alarms be setup to notify the Parole LEADS Security Administrator when anomalous events occur.

The audit function supports accountability by providing a trail of user actions. Actions are associated with individual users for all security relevant events. The audit trail can be examined to determine what happened and which user was responsible for a security relevant event. For each recorded event, the audit record will include the date and time of the event, type of event, offered user ID for unsuccessful logins or actual user ID for other events, and origin of the event (e.g., computer name or IP address).

The Parole LEADS application shall cause a record to be written to the security audit trail for at least each of the following events:

- Failed user authentication attempts
- Resource access attempts that are denied
- Attempts, both successful and unsuccessful, to obtain privilege
- Activities that require privilege
- Successful access of security critical resources
- Changes to Parole LEADS users' security information
- Changes to the Parole LEADS system security configuration or modification of system software

Alarm thresholds should be determined in order to notify the Parole LEADS ISO or Enterprise EIS personnel of potential security violations.

Parole LEADS audit trail records shall be kept for a minimum of three (3) years.

Parole LEADS Agency Service Suspension or Termination Process

If Parole LEADS service to an authorized agency must be suspended or terminated, DAPO shall issue a letter suspending or terminating the agency and its associated end users. This letter will explain the reasons for the suspension or termination and advise the agency that the action can be appealed to the DAPO Director. All authorized user logon identifiers and passwords associated with that agency will be canceled by the Parole LEADS Security Administrator immediately.

If an agency loses CLETS Criminal History capability or is sanctioned by action of DOJ or the CLETS Advisory Committee, that agency will be terminated from Parole LEADS access until such time as the sanctions are lifted.

Parole LEADS Security Incident Escalation Standards

Reporting

It is the responsibility of all users with authorized access to Parole LEADS to report all incidents that would place DAPO information assets at risk. The following incidents shall be reported to the Parole LEADS Security

Administrator or designee at ParoleLEADS2@cdcr.ca.gov:

- Any incidents involving or suspected to involve unauthorized access to Parole LEADS information, automated files, or databases.
- Any incident involving the unauthorized modification, destruction or loss of automated data, automated files, or databases.
- Any incident involving a virus, worm, Trojan horse or other such computer contaminant.
- Any incident involving the unauthorized use of computer equipment, automated data, automated files or databases.
- Any incident involving or suspected to involve the misuse of DAPO information assets.

Security Incident Handling

The Parole LEADS Security Administrator is authorized to respond to any security incidents associated with the operation of Parole

LEADS. The Parole LEADS Security Administrator will review with the Information Security Office all security incidents at the next scheduled meeting for action or for permanent resolution of temporary actions taken by the Security Administrator.

Closure

The Parole LEADS Information Security Office shall be the final authority for closing any actions required for a specific security incident associated with the operations of the Parole LEADS system. An Information Security Incident Report shall be submitted to the Department of Finance in accordance with CDCR DOM IV, Section 49010.6.5 if the incident involved one or more of the following:

- Unauthorized intentional release, modification, or destruction of confidential or sensitive (CORI) information, or the theft of such information including information stolen in conjunction with the theft of a computer or information storage device.
- Use of State Information asset in the commission of a crime.
- Intentional damage or destruction of State information assets, or the theft of such assets with an estimated value in excess of $500.

Parole LEADS Training and Awareness

DAPO shall provide training to the law enforcement community in order to ensure the overall effectiveness, success, and efficiency in operating the Parole LEADS application. Training shall focus on the following items:

- Introduction to Parole LEADS
- Parole LEADS System Overview
- Handling Criminal Offender Records Information (CORI)
- Parole LEADS System Functions
- Search for Parolee Information
- DAPO Parolee Database Download
- Understanding of Parole LEADS Information Sources, Limitations, and Cautions
- Parole LEADS Administrative Structure
- Parole LEADS Security Awareness Issues
- Beware of "Social Engineering"
- The Importance of Protecting Passwords
- Working with the Parole LEADS Security Administrator or designee
- Security Incident Reporting
- Questions and Answers