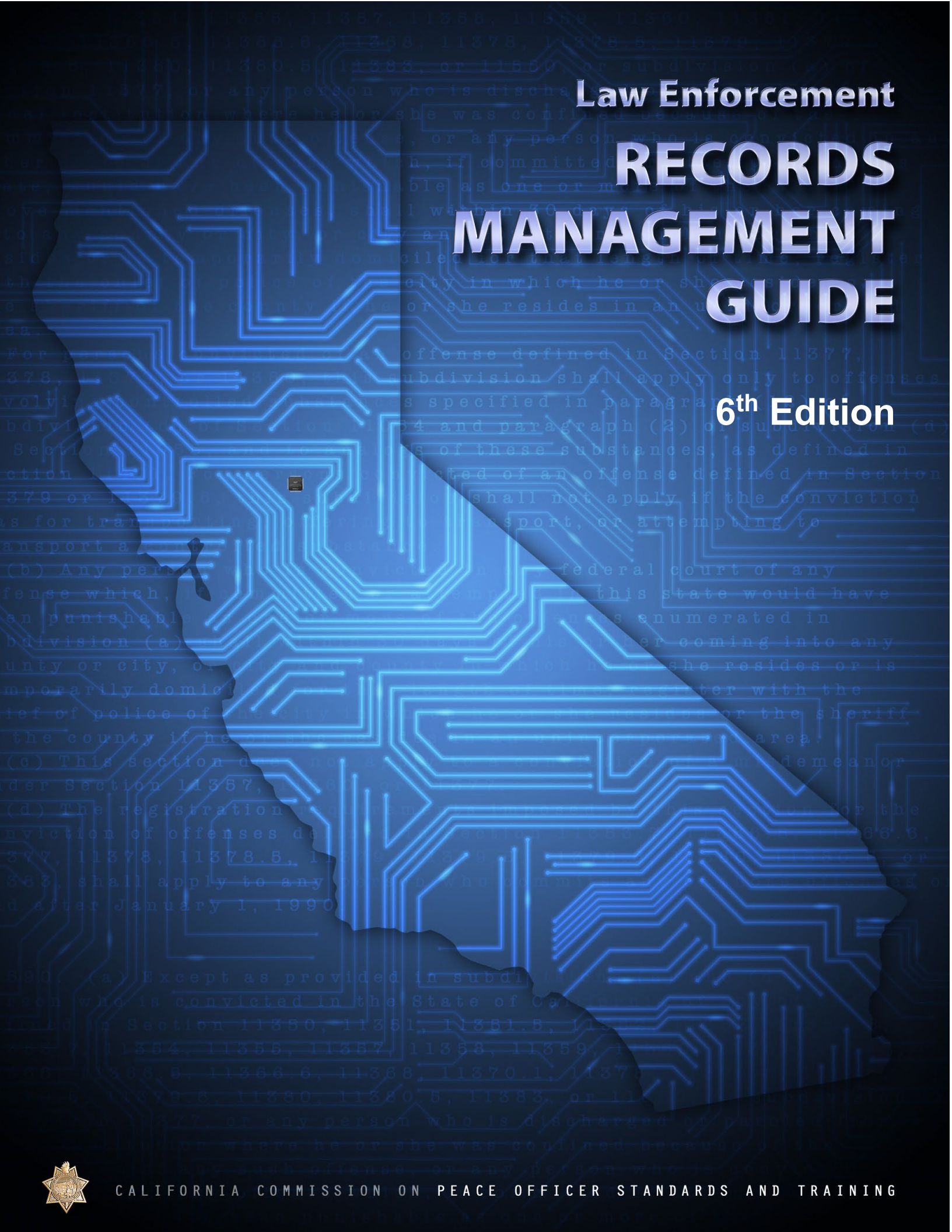
Law Enforcement

RECORDS MANAGEMENT GUIDE

6th Edition



CALIFORNIA COMMISSION ON PEACE OFFICER STANDARDS AND TRAINING

Law Enforcement Records Management Guide

Published January 2014
Updated June 2022

POST MISSION STATEMENT

The mission of the California Commission on Peace Officer Standards and Training is to continually enhance the professionalism of California law enforcement in serving its communities.

POST COMMISSIONERS

Chair
Joyce Dudley
District Attorney, Santa Barbara County

Vice Chair
Rick Braziel
Educator, Humboldt State University

Commissioner
Alan Barcelona
Special Agent, Department of Justice

Commissioner
Ingrid Braun
Sheriff, Mono County

Commissioner
Barry Donelan
Sergeant, Oakland Police Department

Commissioner
P. Lamont Ewell
Public Member, Senate Pro Tempore Appointed

Commissioner
Kelly Gordon
Chief, Santa Barbara Police Department

Commissioner
Geoff Long
Public Member

Commissioner
Tina Nieto
Chief, Marina Police Department

Commissioner
James O'Rourke
Sergeant, California Highway Patrol

EX-Officio Member
Rob Bonta
Attorney General, Department of Justice

Foreword

A law enforcement records management system is a valuable source of relevant information essential to the investigative, arrest, and judicial processes. The failure to manage the records function can affect the successful prosecution of criminal violators, resulting in liability or a loss of public confidence.

The purpose of the Peace Officer Standards and Training (POST) **Law Enforcement Records Management Guide** is to provide standardized resource material for the management of the law enforcement records function, detailing best practices for the receipt, storage, and disposition of records maintained by the agency.

Effective policies and procedures must be established to efficiently manage the law enforcement records function. Agencies should use the information contained in this guide to create or amend policies and procedures to ensure the integrity of the records process.

The Commission on POST intend this guide to serve as a comprehensive resource to aid records personnel, supervisors, managers, and executives in understanding the critical role of the records function to the agency, the criminal justice system, and the community. To ensure its relevance, this guide will be maintained as a living document subject to annual review.

The Commission appreciates the contributions of an ad-hoc advisory committee of records personnel from law enforcement agencies throughout California.

Comments or questions related to the information contained in this guide should be directed to POST at (916) 227-3909.

MANUEL ALVAREZ JR.
Executive Director

Acknowledgments

2021-2022 AD HOC ADVISORY COMMITTEE	**John Dolan**	Foster City Police Department (Ret)
	Tori Hughes	Stanislaus County Sheriff's Office
	Emma Johnson	El Segundo Police Department
	Victoria O'Keefe	San Louis Obispo County Sheriff's Office
	Cerina Otero	Stanislaus County Sheriff's Office
	Joe Surges	Concord Police Department (Ret)
	Christy Witherspoon	Torrance Police Department
POST COORDINATORS	**Robert Ziglar**	
	Larry Ellsworth	
	Michael McHenry	
	Terri Suggett	

Table of Contents

POST MISSION STATEMENT iii
POST COMMISSIONERS iv
Foreword v
Acknowledgments vi
Relevance of the Law Enforcement Records Function x
Navigating the Guide x
Incorporating the Guide into Agency Directives to Meet Best Practices x

1. Organizational Considerations 1
   PURPOSE 1
   Resources 1.1 – Organizational Structure 1
   Resources 1.2 – Personnel Assignment and Training 1
   Resources 1.3 – Personnel Call-Out Procedure and Hours of Operation 2
   COMMENTARY 2
   Resources 1.4 – Emergency and Disaster Preparedness/Personnel Communications/Duress Alarms 3
   Resources 1.5 – Budget Allocation 3
   Resources 1.6 – Policy and Procedure Development 4

2. Primary Report System 6
   Resources 2.1 – Elements of A Primary Report System 6
   Resources 2.2 – Access to Records 10
   Resources 2.3 – Report Distribution Process 11
   Resources 2.4 – Report Numbering System 11
   Resources 2.5 – Records Maintained in Specialized Units 12
   Resources 2.6 – Forms Control 12

3. Secondary Processes 14
   Resources 3.1 – Alcoholic Beverage Control Notification 14
   Resources 3.2 – Bail/Bond Processing 15
   Resources 3.3 – Child Abuse Reporting 15
   Resources 3.4 – Citations 16
   Resources 3.5 – Coroner Records 18

Resources 3.6 – Detention Certificates 19
Resources 3.7 – Disposition of Arrest and Court Action (Adult and Juvenile) 20
Resources 3.8 – Elder and Dependent Adult Abuse 21
Resources 3.9 – Field Interview Cards 21
Resources 3.10 – Fingerprints 22
Resources 3.11 – Firearms 25
Resources 3.12 – Inmate Records 25
Resources 3.13 – Missing Persons 26
Resources 3.14 - Photographs 28
Resources 3.15 – Property 29
Resources 3.16 – Record Sealing 30
Resources 3.17 – Registrant Files 36
Resources 3.18 – Secondhand Dealer and Pawnbroker Licensing 40
Resources 3.19 – Special Incident Reporting Forms for Bombs/Incendiary Devices/Explosives 41
Resources 3.20 – Subpoenas 41
Resources 3.21 – Restraining Orders 42
Resources 3.22 – Vehicles 43
Resources 3.23 – Warrant Processing 44

4. Confidentiality and Release of Information 45
Resources 4.1 – Confidentiality of Records 45
Resources 4.2 – Access to And Release of Agency Records 45
Resources 4.3 – Information Which Must Be Released 46
Resources 4.4 – Exemptions to The Release of Information 48
Resources 4.5 – Public Records Act Response Timelines, Refusals, and Fees 50
Resources 4.6 – Documenting Information Release 50
Resources 4.7 – Collision Reports Release 51
Resources 4.8 – Other Information Release 51
Resources 4.9 – Consequences for The Unauthorized Access of Information 51

5. Statistical Reporting 53
Resources 5.1 – Monthly Mandatory Reporting 53
Resources 5.2 – Uniform Crime Reporting 53
5.2 A - Summary Reporting System 54

5.2 B – California Incident-Based Reporting System (CIBRS) and National Incident Based Reporting System (NIBRS) Crime Classifications 56
Resources 5.3 – Other Mandatory Statistical Reporting 56
Resources 5.4 – Clery Act Reporting 58

6. Records Retention, Purging, And Destruction 60
Resources 6.1 – Records Retention 60
Resources 6.2 – Destruction Resolution/Ordinance Preparation 60
Resources 6.3 – Purge and Destruction of Records 61
Resources 6.4 – Marijuana Records Destruction 62

7. Automation of Records 63
Resources 7.1 – Imaging 63
Resources 7.2 – Live Scan/Cal-ID 63
Resources 7.3 – Personnel, Training, And Capital Expenditure 64
Resources 7.4 – Changes in Workflow and Procedures 65
Resources 7.5 – Feasibility Study 65
Resources 7.6 – Protecting Computer System Files & Resources 72

8. Audits 73
Resources 8.1 – External Audits 73
Resources 8.2 – Internal Audits 74

Glossary 76
Web Resources 81
Legal Reference 85

Relevance of the Law Enforcement Records Function

The *POST Law Enforcement Records Management Guide* was developed as a resource for law enforcement agencies and personnel, noting best practices and resource guide for the various aspects of the law enforcement records function.

Navigating the Guide

This guide is divided into eight chapters:

1. Organizational Considerations
2. Primary Report System
3. Secondary Processes
4. Confidentiality and Release of Information
5. Statistical Reporting
6. Records Retention, Purging, and Destruction
7. Automation of Records
8. Audits

Each chapter begins with a purpose, introducing the chapter material and supporting its relevance. The chapter purpose is followed by POST guidelines based on California and federal law and national best practices. (For more information on national best practices, refer to the Commission on Accreditation for Law Enforcement Agencies, Inc. (CALEA) standards.)

The resource guide was created to standardize the processes and security related to records management. Following each guideline is an in-depth Commentary further explaining and supporting the specified guideline criteria.

The resource guide includes a glossary, web resources, and legal references relating to law enforcement records management. The resource guide and appendices have been provided as an additional reference to assist agency personnel in policy development and legal compliance.

Incorporating the Guide into Agency Directives to Meet Best Practices

The resource guide and supporting Commentary contained in this guide are provided for use as a framework to assist agencies in the development of written directives to document and standardize the processes related to law enforcement records management. Agency directives should incorporate contemporary law enforcement best practices pertaining to law enforcement records management.
Although several guidelines are driven by statute, none of the guidelines are subject to POST compliance or regulation. POST recommends that agencies comply with California statutes, federal law, and national best practices in the management of law enforcement records. Agency executives are ultimately responsible for all records maintained in their facilities and must make executive decisions to standardize processes, ensure legal compliance, and minimize risk.

Comprehensive written directives, standardized practices, and heightened security can fortify an agency's position if the agency must defend its records management function while reducing agency exposure to unwanted scrutiny and liability. Agencies are encouraged to annually review their directives for relevance and secure the necessary initial and ongoing training for records personnel, supervisors, and managers. In addition, agencies should stay current on evolving trends, and keep abreast of legal and regulatory issues related to law enforcement records management.

1. Organizational Considerations

PURPOSE
An agency relies on its records manager, records supervisor, and records personnel to correctly maintain security and control in the records unit. Each agency has responsibility for the receipt, accuracy, retention, management, release, and disposal of law enforcement records. Proper management, an adequate budget, and initial/ongoing training will enhance the efficiency and knowledge of records personnel.

This chapter addresses:
1.1 Organizational structure
1.2 Personnel assignment and training
1.3 Personnel call-out procedure and hours of operation
1.4 Emergency and disaster preparedness/personnel communications/duress alarms
1.5 Budget allocation
1.6 Policy and procedure development

Resources 1.1 – Organizational Structure

Create or amend a written directive outlining the organizational structure of the records management to include, at a minimum, the following:

- *A clearly defined chain-of-command*
- *A formal organizational chart*

COMMENTARY
The directive should clearly delineate the chain-of-command, from the department head to the records personnel. The directive should include an organizational chart showing the reporting relationship and responsibilities of records management within the organization.

Resources 1.2 – Personnel Assignment and Training

Create or amend a written directive addressing personnel assigned to records management to include, at a minimum, the following:

- *Identifying the records manager*
- *Identifying the records manager position as a specialized, mid-management position*
- *Outlining the desired qualifications, applicable certifications, skills, and duties of the records manager, records supervisor, and records personnel*
- *Identifying an initial and ongoing training plan for all personnel assigned to records management to ensure they remain abreast of best practices, current laws, and regulations*

COMMENTARY
Records management is critical to law enforcement, therefore personnel assigned to this function should be clearly designated by job classification. These are technical, specialized positions requiring extensive knowledge of federal, state, and local laws and regulations. It is recommended the records manager be a specialized, mid-management position.

To ensure integrity and security, a background investigation shall be completed on all personnel assigned to the records management. The background investigation must meet the standards set by California DOJ and the FBI, including a fingerprint check (CLETS PPPs 1.9.2 GC 15165).

To better manage agency risk and reduce liability, all records managers/supervisors should complete the POST Basic Records course, Records Supervisor course, and the Public Records Act course. To ensure records personnel remain abreast of best practices and current laws, POST encourages records managers/supervisors to participate in continuing education. The California Law Enforcement Association of Records Supervisors (CLEARS), California CLETS Users Group (CCUG), California Criminal Justice Warrant Services Association (CCJWSA), California Division of the International Association for Identification (IAI), and the California Crime Intelligence and Crime Analysts Association (CCIAA).

POST encourages networking with regional and county agencies (e.g., law enforcement agencies, prosecuting attorneys, courts, city attorneys, county counsels, and other public agencies) to make consistent inter-agency policies, forms, and procedures, to facilitate communication, and to ensure court compliance. This networking provides a legal basis and a framework for managing records in law enforcement agencies.
The POST Records Supervisor Certificate is available to records managers/supervisors who meet the requirements. Further information is available on the POST Website.

Resources 1.3 – Personnel Call-Out Procedure and Hours of Operation
Create or amend a written directive outlining records of personnel call-out procedures and hours of operation to include, at a minimum, the following:

- *Establishing a call-out procedure and process for emergency access to the records unit during times when authorized personnel are not available, during non-business hours (e.g., nights, holidays, and weekends), or any time emergency access is needed*
- *Establishing/publishing public hours of operation* GC 7922.525(a)
- *Establishing internal hours of operation*

COMMENTARY
A call-out procedure should be established for the records manager/supervisor and records personnel to ensure after-hours access. It is important to identify qualified alternate personnel to provide limited emergency access to records. A protocol for emergency access and monitored entry should be created when records personnel are unavailable.

The California Public Records Act (GC 7922.525(a)) requires public hours of operation to be established.

Resources 1.4 – Emergency and Disaster Preparedness/Personnel

Communications/Duress Alarms

Create or amend a written directive (e.g., ensure that records are a component of the agency emergency action plan per USG OSHA 1910.38(a)) outlining the procedures to ensure the continuation of the records management in the event of an emergency to include, at a minimum, the following:

- *Responding to a critical incident requiring immediate action*
- *Ensuring records personnel are equipped with a method of communication and/or a duress alarm in order to contact/alert dispatch and agency supervision in the event of an emergency*
- *Identifying an appropriate alternate records storage and retrieval method*
- *Identifying circumstances necessitating the records of personnel evacuation (e.g., fire, flood, earthquake, hazardous material spill, etc.)*
- *Identifying actions necessary for the removal, security, transportation, and relocation of records and personnel in the event of an evacuation, with consideration for anticipated length of evacuation*

COMMENTARY

The directive should include identification of a temporary alternate site that includes ample room and security to accommodate the records management for an appropriate period of time. Security measures, a tracking system, proper packaging/containers, and chain of custody should be in place to ensure all records are accounted for during removal, transportation, and relocation.

To enhance the safety of records personnel and provide immediate notification during emergencies, records personnel should have communications with a 24/7 dispatch center. During the duration of the emergency, records personnel should be accompanied by appropriate personnel (sworn/armed personnel) for safety purposes.

Resources 1.5 – Budget Allocation

Create or amend a written directive establishing the allocation and distribution of agency funds to include, at a minimum, the following:

- *Records management should be supported by a stand-alone, line-item budget.*
- *The cost associated with maintaining and purging records has an impact on an agency's budget.*
- *Consideration should be given to costs involved with long-term storage of historical and vital records.*

COMMENTARY

The management of records is a critical part of any law enforcement organization and POST recommends it be fully funded to meet the needs of the organization and the community. The organization's budget should identify the records function separately

with a stand-alone, line-item budget. The records manager/supervisor should have input into the records management portion of the budget.

Resources 1.6 – Policy and Procedure Development

Create or amend a written directive establishing manuals outlining the agency policies and procedures regarding law enforcement records management to include, at a minimum, the following:

Structure

a. *General supervision*
b. *Duties and responsibilities of the records manager/supervisor/personnel*
c. *Job descriptions*
d. *Specialized training*
e. *Access and security of records*
f. *Hours of operation*

Records Overview

a. *Records storage*
b. *Records tracking*
c. *Records forms*
d. *Records indexing*
e. *Records specification (e.g., juvenile, adult, sex offender, etc.)*
f. *Records audits*
g. *Records inspections (e.g., IA, other Government agencies, etc.)*

Receipt, Storage, Sealing, Retention, and Purge/Destruction

a. *Chain of custody (written or electronic)*
b. *Submission of reports according to department policy*
c. *Report intake/right of refusal (error correction) and refusal procedure*
d. *Receipt (intake) of records*
e. *Processing reports*
f. *Distribution of reports- to investigations/DA/etc.*
g. *Storage of records*
h. *Access and security of records (hard-copy, electronic)*
i. *Records sealing*
j. *Retention requirements/records retention schedule*
k. *Purge/destruction guidelines/procedures*

Records Release

a. *Resources for the release of records (to include audio, video, photographs)*
b. *Court orders/subpoenas*
c. *Procedures for duplication of records (e.g., discovery requests)*
d. *Public/personal safety during records release*

COMMENTARY
A comprehensive records policy and procedures manual ensures consistency in the process of managing the records function and allows the organization to comply with all associated statutes and best practices.

The manual should provide standards for the training of newly appointed records personnel and identify the responsibilities of personnel regarding the various records management. Compliance with this guideline can reduce agency liability.
Incorporate into policy the requirement for an annual review of all agency policies and procedures related to the records function.

Penal Code (PC) Section 13650 states: Each local law enforcement agency shall conspicuously post on their internet websites all current standards, policies, practices, operating procedures, and education and training materials that would otherwise be available to the public if a request was made pursuant to the California Public Records Act.

2. Primary Report System

PURPOSE
Primary report system as used in this manual, begins with a call for service and ends with a decision to destroy/purge or retain records.

The primary report system in a law enforcement agency is the source of significant information generated and maintained by an agency. This one system provides a broad base of data from which an agency can generate a wide variety of reports on crime analysis/trends, productivity, and agency management.

This chapter addresses:
2.1 Elements of primary report system
2.2 Access to records
2.3 Report distribution process
2.4 Record indexing (numerical and/or chronological)
2.5 Records maintained in specialized units
2.6 Forms control

Resources 2.1 – Elements of A Primary Report System
Create or amend a written directive establishing procedures to ensure all of the elements of the primary report system are addressed to include, at a minimum, the following:

- *Initial data recording*
- *Types of reports*
- *Preparation of reports*
- *Report review, approval, and correction process*
- *Report indexing*
- *Report distribution*
- *Complaint processing*
- *Filing*
- *Crime statistics*
- *Electronic records format/imaging*
- *Records sealing*
- *Purging/destruction*

COMMENTARY
A primary report system should require a minimum number of report forms. Agencies should standardize and formalize the processing of reports with written procedures.

Awareness of the interdependence of the system's components and personnel requirements is a critical element of the efficiency of the system. System objectives should be clearly defined. In addition, a review mechanism is necessary to assure compliance with changing legal requirements.

Initial Data Recording
Most calls for service are initiated through telephone or radio communications. Both are routinely recorded in most agencies and constitute an agency's first record of the event.

These calls are the starting point for the primary report system. Initial data, whether the result of a call for service or employee-initiated activity, should be recorded in a structured format using a unique numbering system (e.g., Computer Aided Dispatch [CAD] event number and/or report number) to assure relevant and uniform data is collected.

Types of Reports
Not all calls for service or employee-initiated activities require a written report. Many activities can be detailed in a CAD incident record. More formal recording of incident information is accomplished via a police report. Two types of reports are recommended: case file reports and incident reports.

Case file reports are those formal, numbered, operational reports which must be prepared to meet legal or internal agency requirements. They are reports of crimes, suspected crimes, traffic accidents, etc. They describe the occurrence and surrounding circumstances, list involved parties, and summarize the activities and observations.

The case file report should include the following documents related to the event:

- Crime report
- Property/Evidence report
- Arrest/booking report
- Supplementary reports
- Supporting documents
- Audio/video recordings, photos, or other media retained

Incident reports record all events, whether or not follow-up action is necessary. Each agency should establish procedures that specify circumstances under which the incident report is to be used in lieu of a case file report.

Preparation of Reports
The primary purpose of a report is to document and transmit information. An effective report preparation system will ensure:

- Prompt completion and review of reports
- Complete and concise reports
- Accuracy of information
- Minimal processing time
- Timely availability of information

To achieve these results, an agency must identify the key factors affecting report preparation, including:

- Personnel time and costs associated with redundant data entry

- Document handling – the number of times a report must be transferred between the writer, reviewer, and records personnel
- Availability of information – the additional time required for report processing
- Quality/accuracy of information – the accuracy of information

Report Review, Approval, and Correction Process
Reports should be reviewed and approved prior to submission to records. When the report is received in records and additional information is needed for processing or corrections are necessary, the report should be returned to the approver with a request for assistance.

Report Indexing
Accurate and rapid information retrieval is essential to an efficient records management system. The indexing process is vital to efficient retrieval. Best practices dictate the most efficient means of locating records is by a master index. The master index should contain, at a minimum, the date, and names of individuals involved in events, cross-referenced to the report number.

Report Distribution
Report distribution is a series of activities to disseminate information to the proper sources. Many of these activities are mandated by law, while others are subject to local practices.

The policy should specify which types of reports should be routed to the various specialized functions or organizational components for follow-up, and those to be distributed outside the agency. These types of reports can include:

- Department of Justice
    - PC 11107 identifies the reports local agencies are required to send to the DOJ.
    - ***NOTE:*** While this law is still in effect, as of the writing of this manual, DOJ does not currently accept many of these reports. Contact DOJ for clarification if necessary.

- California Highway Patrol
    - VC 20008 identifies the traffic accident reports which must be sent to the California Highway Patrol (CHP).
        - Statewide Integrated Traffic Records System (SWITRS)
- Court liaison officer/district attorney/city prosecutor
    - Copies of reports involving an arrest must be sent to the prosecuting attorney for complaint preparation.
    - The handling of reports in the preparation of complaints and warrants is a matter to be established by individual agencies.
- Other agencies
    - The reporting officer may request a copy of a report to be sent to another agency.

- Release of the report must comply with agency report release policy (see Resources 4-1 Confidentiality and Release of Information).
  - Some cases need to automatically be forwarded to other agencies (see next section)

Other federal and state distribution reports include: (see Section 3 - Secondary Processes)

- Federal Bureau of Investigation (e.g., bomb incidents, bank robberies, kidnappings)
- U.S. Secret Service (counterfeiting)
- Department of Motor Vehicles (e.g., Admin per se)
- Alcoholic Beverage Control (alcohol-related incidents)
- Child Protective Services (child abuse)
- Adult Protective Services (elder abuse)
- Local schools (e.g., employee arrests, on-campus incidents)
- State Board of Control: Victim Witness Program; California Constitution, Article I, Section 28(b) – Marsy's Law

Complaint Processing

Complaint processing is the preparation of documents necessary to file a complaint in a court of law. For further reference, including definition, wording, procedure, and requirements, see PC sections:

- PC 691 provides definitions of felony, misdemeanor, and infraction
- PC 806 provides the definition of felony complaints and proceedings
- PC 853.5 provides information on processing infractions
- PC 853.6 provides information on processing misdemeanors
- PC 859 provides information on processing felonies

Electronic Records Format/Imaging

Ensures the agency complies with the uniform statewide standards adopted by the Secretary of State, in consultation with the Department of General Services, for use in recording, storing, and reproducing permanent and nonpermanent documents or records in electronic media. These regulations list minimum standards recommended by the American National Standards Institute (ANSI) or the Association for Information and Image Management (AIIM) and provide specific conditions that would meet the definition of a trusted system, as provided in GC 12168.7.

As described in the Uniformed Electronics Transactions Act (UETA): "Electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities. "Electronic record" means a record created, generated, sent, communicated, received, or stored by electronic means. (Cc 1633)
Additional resources include:

- CCR 22620.7 Trustworthy Electronic Document or Record Preservation
- GC 10295 Electronic Records
- PC 1546 Electronic Communications Privacy Act
- PC 13103 Electronic Records Destruction

Filing
See Resources 2.2 – Access to Records, below.
Crime Statistics
Refer to Section 5 – Statistical Reporting
Record Sealing
Refer to Resources 3.16, Record Sealing
Purging/Destruction
Refer to Section 6, Records Retention, Purging, and Destruction, for detailed information on record purging and destruction.

Resources 2.2 – Access to Records

Create or amend a written directive addressing access to records to include, at a minimum, the following:

- *Individuals authorized access to the restricted records unit*
- *Process for controlling access to records*
- *Procedures to identify all files and their contents*
- *Method used to file and retrieve documents*
- *Statutory requirements*

COMMENTARY
To ensure security and integrity, agencies need a written directive outlining access to records. Access to the records unit should be limited to authorized personnel only. A log should be maintained noting all non-assigned personnel who have been granted access to the records unit and the reason for access. Non-assigned personnel should not be in the records unit without escort by the records personnel. The agency head or designee should issue, track, and recover any keys or key cards to the restricted area if access is revoked.

Electronically stored data should have security/audit tracking of document viewing, editing, and printing as a component of the records system.
Hard-copy reports should be centralized, conveniently located, and arranged for easy retrieval. Only records personnel should have access to the files. After reports are submitted to records for processing, reports should not be removed from the records work area by non-records personnel. Records personnel who are authorized to remove a hard-copy report from the files should place an out-card in the file identifying the report and where it can be located. Reports should not be maintained at individual workstations.

Within electronic records systems, security settings should be established to allow only authorized personnel access to read, edit, and print reports to maintain an audit trail. Only a few authorized persons should be granted delete rights.
Reports approved by a supervisor and submitted to records for filing and distribution should not be modified or altered except by way of the supplemental report. Approved

reports not yet submitted to records should only be corrected or modified by the author, with the authorization of the reviewing supervisor

Resources 2.3 – Report Distribution Process

Create or amend a written directive establishing procedures for a report distribution process to include, at a minimum, the following:

- *Number of copies sent/needed*
- *Timeliness of distribution*
- *Method of distribution (paper or electronic)*
- *Quality of reproduction process*
- *Time required to prepare report copies*
- *Additions/deletions from standard distribution lists*
- *Annual audit of the report distribution process*

COMMENTARY

A formalized report distribution process ensures consistency and adherence to applicable laws and regulations (see Section 4, Confidentiality and Release of Information).

The agency should conduct an annual review of the report distribution process to maintain effectiveness.

Resources 2.4 – Report Numbering System

Create or amend a written directive establishing a report numbering system to include, at a minimum, the following:

- *Provisions for the assignment of a unique number to every report*
- *Process to ensure no numbers are omitted or duplicated*
- *Identification of any events (e.g., traffic citations) that do not require a report number*

COMMENTARY

A single numbering series should be used for all reports documented by the agency, including traffic collisions, crime reports, and miscellaneous non-criminal reports. The most straightforward report numbering system consists of the last two digits of the current year and a sequential number (e.g., 22-0001, 22-0002) or the entire year and a sequential number (e.g., 2022-0001, 2022-0002). All documents relating to a single event should have this uniform number.

A chronological numbering system may be used. An example of this may be 22-0304-001 (the year 2022, March 4th, first report of the day).

The numbering system should be designed in such a manner that all cases receive either a sequential or chronological number, no numbers are omitted, and no numbers are duplicated. Best practices dictate the agency establish a monthly review process to ensure accountability.

Some activities, such as the issuance of traffic citations, need not be recorded as numbered cases; the citation form itself serves as the report.

Resources 2.5 – Records Maintained in Specialized Units

Create or amend a written directive specifying those records to be maintained in agency specialized units. The directive should address, at a minimum, the following:

- *Case files on active cases*
- *Intelligence records (e.g., vice, drug, organized crime, gang, etc.)*

COMMENTARY

The written directive should specify the types of records and the retention schedules for records maintained in specialized units. For example, criminal investigators should maintain case files on active cases being investigated, to be transferred to records when the investigation is complete. Specialized units may be permitted to maintain records independently for additional security and control.

Resources 2.6 – Forms Control

Create or amend a written directive establishing a forms control process to include, at a minimum, the following:

- *Identification of a forms control custodian*
- *Procedure for creating/revising forms*
- *Utilization of federal, state, and local forms*
- *Automated forms management*

COMMENTARY

A forms control process is designed to ensure uniformity and compliance with federal law, state law, local ordinances, and department policy. The process is designed to prevent the creation and use of unauthorized forms and to identify and discontinue use of forms deemed no longer necessary.

Identification of a Forms Control Custodian

Identify and specify the responsibilities of a forms control custodian, which should minimally include establishing uniformity, compliance, training, and removal of obsolete forms.

Procedure for Creating/Revising Forms

Establish a schedule for the regular review of agency forms to ensure the most up-to-date information is being captured in compliance with federal law, state statutes, department policy, and records management system (RMS) vendor updates. The form number and creation/revision date should be displayed on all forms. During the review process, agencies should determine whether the form is still necessary.

Utilization of Federal, State, and Local Forms

Required state forms may be found on state websites (e.g., California Law Enforcement Website [CLEW], the California Courts, the California Attorney General, US Department of Justice, and the California Department of Motor Vehicles [DMV]).

CLEW, maintained by the DOJ, requires user registration to obtain access to forms. Although any agency personnel member may register with CLEW, it is particularly important the forms control custodian has access to receive updates as they occur. Local forms (e.g., juvenile contact reports, field interview [FI] cards, administrative citations, etc.) include those developed by an agency or a local jurisdiction.

Automated Forms Management
Not all forms will be in hard-copy format. Some forms can be completed in electronic format, such as PDF or Word templates. The forms control custodian should ensure consistency, uniformity, and compliance with federal law, state statutes, local ordinances, and agency policy.

3. Secondary Processes

PURPOSE
This chapter provides guidance on secondary processes used in law enforcement records.

This chapter addresses:
3.1 Alcoholic Beverage Control notification
3.2 Bail/Bond processing
3.3 Child abuse reporting
3.4 Citations
3.5 Coroner records
3.6 Detention certificates
3.7 Disposition of Arrest and court action (Adult and Juvenile)
3.8 Elder and dependent adult abuse
3.9 Field Interview cards
3.10 Fingerprints
3.11 Firearms
3.12 Inmate records
3.13 Missing persons
3.14 Photographs
3.15 Property
3.16 Record sealing
3.17 Registrant files
3.18 Secondhand dealer and pawnbroker licensing and reporting
3.19 Special incident reporting forms for bombs/incendiary devices/explosives
3.20 Subpoenas
3.21 Restraining Orders
3.22 Vehicles
3.23 Warrant processing

Resources 3.1 – Alcoholic Beverage Control Notification

Create or amend a written directive establishing a process for providing notification to the Department of Alcoholic Beverage Control (ABC), within 10 days of the following:

- *Arrests for any violation of state, city, or county laws occurring on an ABC-licensed premise, or an immediately adjacent area under the control of the licensee*
- *Arrest of a licensee occurring on or off the licensed premises, or of any person for illegal sale, manufacture, or possession of alcoholic beverages*

COMMENTARY
Business and Professions Code (BP) section 24202 requires mandatory notification of arrests to ABC by all state and local law enforcement agencies, within 10 days.
Law enforcement is encouraged to track and compile additional statistics on drug and alcohol involvement in any type of incident via NIBRS/CIBRS.

Resources 3.2 – Bail/Bond Processing

Create or amend a written directive for processing bail/bond to include, at a minimum, the following:

- *Verify the bond/warrant*
- *Verify the bail agent license*
- *Process the bond*

COMMENTARY

Local agencies who accept bail or bond should have detailed specific personnel responsibilities to process bail/bond on any warrant, case, or charge for those who are eligible. The initial steps should include verification of the case, the charges and or warrant and licensing confirmation of the bail agent and verification of the defendant's eligibility for bail or bond.

Verify and accept the bond. A copy of the bond must be included in the court package. The original bond has to be forwarded to the court.

For cash bail, count the money and issue a receipt. The agency should forward the funds via check to the court. A copy of the receipt must be included in the court package.

If applicable, make appropriate notifications regarding the release of the defendant.

Resources

- *California Department of Insurance verification of license status*
- *PC 1268-1320.5 Defines bail processes*

Resources 3.3 – Child Abuse Reporting

Create or amend a written directive detailing procedures for child abuse reporting to include, at a minimum, the following:

- *Reporting requirements*
- *Reporting instructions*

COMMENTARY

PC 11165.6 defines child abuse as a physical injury that is inflicted by other than accidental means on a child (a person under the age of 18 years) by another person. It means the sexual abuse of a child or any act or omission proscribed by PC 273a or 273d, and the neglect of a child or abuse in out-of-home care as defined in PC 11165.5. For further information, see PC sections 11165.1-11165.6.

The applicable code sections include, but are not limited to:

- PC 261 Rape
- PC 261.4 Rape of an unconscious person
- PC 261.5 Statutory rape
- PC 264.1 Forcible sex in concert with another

- PC 266(c) Induce intercourse/sex acts by false representation with intent to create fear
- PC 273a Child endangerment
- PC 273d Willful cruelty to a child
- PC 285 Incest
- PC 286(b)(1)(c)(d) Sodomy of a person under 18 years of age
- PC 287 Oral copulation of a minor
- PC 288 Lewd and lascivious acts on a child under 14 years of age
- PC 288.5 Continual sexual abuse of a child under 14 years of age
- PC 289(a) Forcible penetration with a foreign object
- PC 647(a) Lewd conduct
- PC 647.6 Annoying or molesting a child under 18 years

Reporting Requirements
DOJ Information Bulletin 11-10-BCIA, found on CLEW, contains additional information regarding reporting requirements.

PC 11169 requires a child protective agency to report every suspected incident of child abuse it receives to another child protective agency in the county, the agency responsible for investigations under WI 300, and the prosecuting attorney's office. Reporting with telephone notification is to be made immediately or as soon as is practical. Written notification shall follow within 36 hours of receiving information concerning the incident.

Reporting Instructions
The DOJ requires child abuse to be reported on form BCIA 8583, "Child Abuse Investigation Report." This form is available in the Child Abuse Central Index Form section of the California Attorney General's Website.

Resources 3.4 – Citations

Create or amend a written directive detailing procedures for processing citations to include, at a minimum, the following:

- *Types of citations*
- *Transmittal of citations to court*
- *Citation processing*
- *Voiding moving/parking citations*

COMMENTARY
The California Judicial Council has defined the basic format for the "Notice to Appear," however, there are local options in citation forms. All current citation formats are available separately on the California Courts Website. The document can also be found at Notice to Appear and Related Forms.

When using automated systems, entering citation information provides crime analysis data and allows citations to be readily available.

Types of Citations
On a monthly basis, most agencies analyze the number and type of citations written by field personnel. The most common citation categories are hazardous (moving), non-hazardous (non-moving/equipment), parking, non-traffic misdemeanor, administrative and other. An agency may use other categories. Citation data is used for both operational and administrative decision making.

A copy of each citation should be filed in records according to the retention schedule. There are a variety of filing methods for citations. In determining the best method, it is necessary to know how the citations are accessed.
The most common reasons for retrieving a citation are:

- The defendant lost the citation and needs information.
- An officer has received a subpoena and needs a copy of the citation. The subpoena may not include the citation number but will include the defendant's name.
- Administrative hearings.
- Purging according to the agency retention schedule.

Transmittal of Citations to Court
Citations should be sent to the court in a timely fashion. Local policies will dictate the method by which citations are sent to the court.

Citation Processing

- Misdemeanor citations: Some counties permit minor misdemeanor citations to be directly transmitted to the court. Others require a report to supplement the information on the citation. Consult with the prosecuting attorney to establish local policy. File a copy of the citation with the report. The agency copy of the citation can be filed in the citation file.
- Vehicle Code: Vehicle Code (VC) offenses involving moving citations are processed through the local court system. Contact the court clerk for processing information.
- Juvenile Citations: Juvenile misdemeanor citations usually are sent to juvenile probation with a copy of the offense report. A copy of the citation is attached to the original offense report. If using an automated RMS system, the citation may be entered into the citation section of the system prior to being filed in the citation file. Some agencies utilize a juvenile diversion program where they handle juvenile citation in-house. Check your local court procedures for further information on juvenile traffic citations.
- Administrative citations: Administrative citations are sent to the city attorney. Within the city attorneys' office, there is a hearing officer with whom an appeal may be made, or the fine may be paid. A copy of the citation is filed in the citation file.
- Notice of correction citations: In many instances, the driver will correct the deficiency and return to the law enforcement agency to have the violation "signed-off" on the driver's copy. This may be done by an officer or other authorized employee. For information regarding fees allowing sheriff's offices to

charge for services, refer to GC 26746.1. The courts and/or local agencies may impose a fee for this service. The agency copy of the citation can be filed in the citation file.

- Citation amendments: If an error is found on a citation, a Judicial Council form TR100, Notice of Correction and Proof of Service, is completed with the correct information, and a copy is mailed to the defendant. The original is sent to the court and the agency keeps a copy, which is filed with the citation.

Each agency must establish a policy for indicating "booking required" pursuant to PC 853.6(g) when issuing a citation for recordable offenses (e.g., PC 488 petty theft, 240 simple assault, 415 disturbing the peace, etc.).

PC 853.6(g) provides for fingerprinting of misdemeanor defendants prior to court appearances. An officer may book the arrested person prior to release. Or the officer may indicate on the citation that the arrested person shall appear at the arresting agency to be booked or fingerprinted prior to court. The arresting agency at the time of booking or fingerprinting shall provide the arrested person with verification (a receipt or entry on the citation) of the booking or fingerprinting.

If the citation indicates the arrested person is to be booked or fingerprinted, the court is required to order the defendant to provide verification of the booking before the proceedings begin. If no verification is provided, the court may require verification at the next court appearance.

Parking Citations
Parking citations are a form of administrative citations which are not submitted to court. A person may request an initial review of the citation by the issuing agency. The issuing agency or the processing agency shall communicate the results of the initial review to the person contesting the notice. If a person is not satisfied with the results of the review, the next step in the process is to request an administrative hearing.

Voiding Moving/Parking Citations
VC 40202(a) contains specific language which will allow a law enforcement agency to cancel a citation after it has been written.
VC 40202(a)(c) and GC 6200 admonish law enforcement personnel for the illegality of altering a citation before it is filed with the processing agency.

Resources 3.5 – Coroner Records

Create or amend a written directive detailing procedures addressing coroner records to include, at a minimum, the following:

- *Where to maintain coroner records (separate from law enforcement records)?*
- *Which records become public records and when?*
- *Which records are not public records?*

COMMENTARY
Coroner records are defined as those documents which record the investigation into the manner and cause(s) of death.

Although there is no state standard, a sheriff-coroner agency should file coroner records within their coroner function and not within law enforcement records in order to avoid a possible conflict of interest. Coroner records should be maintained in coroner report number order. The subject's name can be included in the agency's master index file, cross-referenced to the coroner's report number.

After the death certificate has been finalized, the four records listed below become public information and copies can be obtained at a cost that should be established by ordinance.

- Toxicology report
- Autopsy report
- Coroner's report
- Death certificate (a certified death certificate is accessible only by authorized persons per Health and Safety Code [H&S] Section 103526)

Additional records may be generated during a coroner's investigation.
The following records are ***NOT*** public:

- Law enforcement reports, unless determined by the law enforcement agency to be public information under GC 6254(f) or appropriate local "sunshine ordinance"
- Criminal history records which are obtained after the submission of fingerprints to DOJ
- Photographs of the decedent pursuant to California Code of Civil Procedures Section (CP) 129

Photographs may be used in a criminal action or proceeding which relates to the death of that person. A court order may be necessary to release the photographs.
Records personnel should check with the prosecuting attorney's office and/or the appropriate investigation unit prior to releasing information during an open criminal action or proceeding.

Resources 3.6 – Detention Certificates

Create or amend a written directive detailing procedures for processing detention certificates to include, at a minimum, the following:

- *When to issue detention certificates*
- *Detention when no accusatory pleading is filed*
- *DOJ notification of detention only*

COMMENTARY
Pursuant to PC 851.6(a), when a person is arrested and released pursuant to paragraphs (1) or (3) or PC 849(b), the person shall be issued a certificate, signed by the releasing officer or his/her superior, describing the action as a detention.
In a case where a person was arrested and released, and no accusatory pleading was

filed, the person shall be issued a certificate by the law enforcement agency which arrested him/her describing the action as a detention. The law enforcement agency will be notified of the filing rejection upon return of the Disposition of Arrest and Court Action form (JUS 8715) from the prosecuting attorney.

The form and content of the detention certificate shall be prescribed by the Attorney General. See CLEW for the most updated forms.

The law enforcement agency must update its records and notify DOJ so any reference to the action shall refer to it as a detention, not an arrest (refer to PC 851.6(d]).

Resources 3.7 – Disposition of Arrest and Court Action (Adult and Juvenile)
Create or amend a written directive detailing procedures for processing adult and juvenile disposition reporting forms to include, at a minimum, the following:

- *When to initiate form*
- *Required information reporting*
- *Include form with case documentation*
- *Submit form to DOJ within 30 days of disposition*

COMMENTARY
The Disposition of Arrest and Court Action form (JUS 8715) and the Juvenile Detention Disposition Report form (JUS 8716) is used to report the disposition of an arrest, warrant arrest, indictment, and/or subsequent action(s) to the DOJ for each offense. This form must be included with the case documentation and stay with the case as it proceeds through the criminal justice system from point of arrest to final adjudication. (NOTE-As of July 1, 2022, all law enforcement and prosecution level dispositions must be submitted utilizing the web form via the Criminal Justice Data Exchange [CJDE]).

Initial Procedures
The arresting agency is responsible for initiating and reporting all information in Section A (Law Enforcement Information) on the JUS 8715 and JUS 8716 forms (or electronic equivalent) for all arrests involving recordable offenses. The arrest information must be the same as that submitted via Live Scan, fingerprint record, or as indicated on the citation. The form must be included with the case documentation when it is submitted to the prosecutor or the court. This includes:

- Citations
- On-view arrests
- All warrant arrests

Even when the defendant is not fingerprinted for a recordable offense, a JUS 8715 or JUS 8716 form must be initiated. Although the arrest and disposition data will not be entered into the criminal history record, the information will be used by the Bureau of Criminal Information & Analysis/Law Enforcement Information Center (LEIC).
The JUS 8715 or JUS 8716 form must be submitted to the DOJ within 30 days after disposition pursuant to PC 11115 and 13151 either electronically through Justice Automated Data Exchange (JADE) or to the address shown on the back of the form.

Criminal Justice Data Exchange (CJDE) is available to law enforcement and prosecuting attorneys to submit arrest level information.

Forms may be obtained via CLEW. The DOJ can provide forms to be completed manually or forms that feed through automated printers.

The *Arrest and Disposition Instruction Manual* is available on CLEW (Publications – Manuals, Guides, Codes, and Tables). The DOJ Field Operations Unit, Arrest and Disposition Training Unit, provide training on the proper completion of the form.

Resources 3.8 – Elder and Dependent Adult Abuse

Create or amend a written directive detailing procedures for processing elder and dependent adult abuse forms to include, at a minimum, the following information:

- Report requirements
- Reporting instructions

COMMENTARY

The following statutes define elder (WI 15610.27), dependent adult (WI 15610.23), and abuse (WI 15610.07).

Reporting Requirements

WI 15630(a) requires certain professional occupations, including law enforcement agencies, to report cases of elder and dependent adult abuse to designated authorities. When reporting elder and dependent adult abuse, WI 15630 requires the mandated reporter to report the known or suspected abuse within specified time frames as outlined in this section. A report is required for each incident and each victim.

Reporting Instructions

Suspected elder or dependent adult abuse is reported on Form SOC341, Report of Suspected Dependent Adult/Elder Abuse. This form can be obtained from the county adult protective services agency.

Ensure other information is complete as required by WI 15630(e) which is the reporting requirement.

Resources 3.9 – Field Interview Cards

Create or amend a written directive detailing procedures for processing field interview cards to include, at a minimum, the following:

- *Filing of hard-copy field interview cards*
- *Access to field interview cards*
- *Retention/destruction of field interview cards*

COMMENTARY
A field interview (FI) card is used to record suspicious or unusual circumstances, persons, vehicles, or events. The primary purpose of an FI card is to document activity in a particular location at a specific time. The agency's legal advisors should be consulted regarding the retention of juvenile information and photographs obtained as part of a field interview.

Filing of Hard-Copy Field Interview Cards
Hard-copy FI cards should be filed chronologically, with the most recent cards in the front of the file. As new cards are filed, the older cards should be moved to the rear of the file, still in chronological order. Alphabetical filing defeats the chronological reference use of the cards.
The date, time, and location of the field interview should be placed on the top line of each FI card. This facilitates filing and retrieval of the card.

Access to Field Interview Cards
If an agency uses manual indexing and processing for hard-copy FI cards, the cards should be maintained in a secure location. Identify specific personnel within your agency who should have the responsibility to keep the file current and assist with searches and the retrieval of information.
Automated record systems simplify the processing of FI cards. The cards do not need to be retained in the records unit after data entry as the information from the cards is available to all authorized users electronically. This allows the card to be maintained by investigation and crime analysis personnel for use in relation to gang tracking and special investigations.

Retention
FI cards should be maintained until destroyed per the agency record retention schedule.

Resources 3.10 – Fingerprints

Create or amend a written directive detailing procedures for processing fingerprints to include, at a minimum, the following:

- *Criminal fingerprints*
- *Applicant fingerprints*
- *Registrant fingerprints*

COMMENTARY
Law enforcement agencies use fingerprints to identify subjects of criminal investigations, licensing, certification, employment, and general identification purposes.

Legal Mandates
PC 13150 requires the reporting agency, for each arrest, to report to the DOJ the applicable identification and arrest data described in PC 13125. This requirement includes fingerprints and the Disposition of Arrest and Court Action form (JUS 8715).

California Identification System (Cal-ID)
The California Identification System (Cal-ID) is a statewide, multi-database system that allows local law enforcement agencies to have varying levels of access for ten-print and latent print identification purposes.

Cal-ID comprises four (4) individual databases:

- Automated Fingerprint Identification System (AFIS): This system consists of minutiae data for the right and left thumbs for purposes of conducting searches of inked fingerprints. This is referred to as a ten-print search.
- Automated Latent Print System (ALPS): This system consists of minutiae data for eight fingers (right and left little fingers are currently omitted) of specified felony-level offenders and is used for conducting searches of latent prints from crime scenes or physical Evidence.
- Latent Database (LDB): This database consists of minutiae data of latent prints searched against the ALPS database and not identified. New offenders who are registered to the ALPS database are automatically searched against this unsolved latent file to identify first-time arrestees for offenses committed prior to their arrest.
- Digital Image Retrieval System (DIRS): This system consists of side-by-side images of all fingers registered to the AFIS or ALPS databases and patents registered to the LDB.

There are various services in the Cal-ID system. Refer to *Guidelines for Submitting Applicant Live Scan Transactions* and *Guidelines for Submitting Criminal Live Scan Transactions,* available on CLEW, for further information.

Live Scan
Live Scan devices electronically capture fingerprint images and arrest data at the point of booking. Live Scan eliminates the use of ink in fingerprinting and allows an operator to print as many copies as necessary after completing the booking.
Live Scan fingerprinting is used for three types of printing: (1) adult criminal, (2) juvenile criminal, and (3) applicants.

Criminal Fingerprints
Arrest fingerprints must be submitted to the DOJ Bureau of Criminal Identification and Information (BCII) to establish a criminal record within DOJ. To add an arrest entry to an existing criminal record, fingerprint impressions must be submitted to DOJ. This is required by DOJ for *each* arrest made to ensure identification can be made.
Offenses include:

- On-view arrest
- Warrant arrest
- Supplemental and/or additional arrest
- Court-ordered booking or book and release
- Commitment prints (California Department of Corrections and Rehabilitation [CDCR], local law enforcement agencies)
- Deceased prints submitted by the coroner pursuant to PC 11109

- Probation department prints when the subject has no prior criminal record within DOJ, or to register a probation or diversion notice

Accompanying arrest dispositions (JUS 8715 manual forms or automated format) must be created and submitted to DOJ to eventually complete the arrest cycle on the Record of Arrest and Prosecution form (rap sheet).

Fingerprints may be submitted to BCII on subjects for identification purposes only that have "Question of Identity" or "For Inquiry Only" indicated in the charge area. Fingerprints will be searched through BCII records. Results will be returned to the submitting agency.

DOJ requires agencies to submit fingerprints and dispositions on all arrests involving juveniles. Dispositions should always be noted. If a disposition is not listed, the charge information will not be released. Sample dispositions include:

- Petition requested
- Release to parent
- Release to parent/petition requested
- Counseled and released (including police probation)
- PC 849, 849(B), or 849(B)(1) – release from custody without charge
- Non-detained petition
- Detained petition
- Juvenile Hall

Applicant Fingerprints

BCII provides edited summary criminal history information for employment, licensing, and certification purposes (PC 11105). Records personnel should refer to the DOJ *Live Scan Manual*, available on CLEW, for information on submitting requests, forms to be used, fees, level of service, and other pertinent information. DOJ now offers an applicant expedite service for an additional fee.

All requests for criminal history information must be submitted via Live Scan. DOJ provides a "subsequent arrest notification service" to all law enforcement and contracting agencies on employees. Pursuant to PC 11105.2(c), (d), (e), and (f), a "no longer interested" form must be completed and submitted electronically to DOJ on a subject previously fingerprinted for employment, licensing, or certification. This form is found in the *DOJ Applicant Fingerprint Clearance Manual* available on CLEW.

Registrant Fingerprints

Certain persons are required to register pursuant to PC 290 (sex offenders), PC 186.30 (gang offenders), and PC 457.1 (arson offenders). The agency having jurisdiction over the subject's place of residence is responsible for the registration process. Registrations require fingerprints to be submitted to the DOJ Registration Unit.

Fingerprint Cards

Criminal Fingerprint Cards (FD-1164) can be ordered from the FBI. There is no fee for

the cards. Include the agency's name, mailing address, and NCIC ORI number in the order.

Federal Bureau of Investigation
Logistical Support Unit (LSU), CJIS Division
1000 Custer Hollow Road
Clarksburg, WV 26306
Phone: 304-625-3983; Fax: 304-625-3984

Resources 3.11 – Firearms

Create or amend a written directive detailing procedures for entering firearms information into the CLETS (Automated Firearm System [AFS]) system to include, at a minimum, the following:

- *Circumstances necessitating CLETS (AFS) entry*
- *Identify personnel responsible for entry*

COMMENTARY

Firearms can be entered by records, dispatch, or property and Evidence personnel at agency discretion. For entry instructions, see the CJIS/CLETS manual available on CLEW.

PC Section 11108.2. Requires a law enforcement agency to enter or cause to be entered into the DOJ Automated Firearms System each firearm that has been reported stolen, lost, found, recovered, held for safekeeping, surrendered pursuant to Section 28050, relinquished pursuant to Section 6389 of the Family Code, or under observation, within seven calendar days after being notified of the precipitating event.

PC section 11108.3. Requires law enforcement agencies to enter guns that were illegally possessed, used in a suicide, used in a crime, or suspected of having been used in a crime within 7 days.

For more detailed information on firearms and the laws Governing them, see the POST Law Enforcement Evidence & Property Management Guide.

Resources 3.12 – Inmate Records

Create or amend a written directive establishing procedures for the maintenance of inmate records in accordance with state laws and regulations to include, at a minimum, the following:

- *Records classification*
- *Information to be maintained*

COMMENTARY

Local detention facilities must maintain certain inmate records, depending upon the record's classification. PC 6030 authorizes the State Board of Corrections (BSCC) to enforce regulations for local detention facilities.

The California Code of Regulations (CCR), Title 15, Chapter 1, Subchapter 4, section 1041 describes what information must be maintained in regards to inmate records. Sections 3260-3379 can provide further information on inmate records.

Records personnel should consider ensuring custody division personnel will facilitate the collection of deoxyribonucleic acid (DNA) samples from arrestees, inmates, or offenders as required by and for submission to the CA DOJ for inmates and probationers in accordance with PC 296.

Resources 3.13 – Missing Persons

Create or amend a written directive establishing procedures for missing person reports to include, at a minimum, the following:

- *Reporting/time requirements*
- *Transmitting reports to California DOJ and NICIC*
- *When the missing person is under the age of 21*
- *When the missing person is an adult*
- *Transmitting reports to other jurisdictions*

COMMENTARY

PC 14200-14215 the Missing Person Reporting Law, assigns responsibility for this subject area to the DOJ Missing/Unidentified Persons Unit (MUPS), local agencies, and CHP.

Reporting Requirements

Departments must:

- Accept any report of a missing person, as defined by PC 14212(a), without delay, regardless of jurisdiction
- Accept any report of a runaway without delay
- Accept reports of missing persons by telephone
- Assign priority to missing person reports over non-emergency property crimes
- Make an immediate assessment of steps to locate based on: type of missing person case, defined in PC 14212(a), and indications that victim might be at risk, PC 14212(d).
- Broadcast a “be-on-the-lookout” bulletin (BOLO) without delay within your jurisdiction if the missing person is under 21 years of age or a person of any age considered “at risk.” (MUPS/CLEW) If the missing report meets the criteria for an Amber Alert or a Silver Alert, ensure proper requests have been made. GC 8594
- If the person reported missing is under 21 years of age, or if there is evidence that the person is at risk, the law enforcement agency receiving the report shall, within two hours after the receipt of the report, electronically transmit the report to the DOJ via the California Law Enforcement Telecommunications System (CLETS) for inclusion in the Violent Crime Information Center and the National Crime Information Center (NCIC) databases.

In accordance with Title 34, United States Code, Section 41307 (Suzanne's Law), a record for a missing person under the age of 21 must be entered into NCIC by federal, state, and local law enforcement agencies. In addition, the Adam Walsh Child Protection and Safety Act of 2006 mandates entry of those individuals into the NCIC within 2 hours of receipt of the minimum data required to enter an NCIC record.

In addition to the above requirements, the CHP:

- May accept reports of missing persons/runaways
- Must immediately advise (PC 14211[b]) the person making the report of the name and phone number of the agency having jurisdiction over the missing person's residence and the location where the missing person was last seen
- If the person making a report of a missing person or runaway, contact the CHP by telephone. The CHP may take the report and shall immediately advise the person making the report of the name and telephone number of the police or sheriff's department having jurisdiction of the residence address of the missing person and of the name and telephone number of the police or sheriff's department having jurisdiction of the place where the person was last seen. (PC 14211).

Transmitting Reports to California DOJ and the National Crime Information Center (NCIC)

Law enforcement agencies taking the initial report must submit the report to DOJ through the California Justice Information System (CJIS) Missing/Unidentified Persons System (MUPS).

PC 14211(e) requires all missing persons to be entered in NCIC. Entry of a missing person into the "MUPS" system will automatically generate an entry into the NCIC Missing Persons System.

Education Code (EDC) Section 49068.6 requires law enforcement to notify the school in which a missing child is enrolled. The school shall flag a missing child's record and immediately notify law enforcement of an inquiry or request for the missing child's records.
Agencies must enter a missing person record into MUPS, even if the missing person is found before the entry is made. In such a case, the agency should enter the missing person record and immediately remove it (e.g., clear the record). (CLEW)
PC 14211-14215 defines a uniform standard on how agencies should be handling these cases. Federal law (Title 34 USC 41308 [Adam Walsh Protection Act], and 41307,) require each federal, state, and local law enforcement agency to report, within two hours, each case of a missing person under the age of 21 to NCIC.

When receiving a missing person report:

- The law enforcement agency must provide the reporting party with DOJ form BCIA 4048, (available on CLEW), "Authorization to Release Dental/Skeletal X-rays, Photograph, and Description Information," which authorizes release of these records.
- The law enforcement agency must submit the missing person information to DOJ within two hours after accepting the report using the CJIS/CLETS System (MUPS) if under 21 or considered "at-risk" (PC 14211(e)).
- The law enforcement agency may execute a written declaration authorizing the release of dental/skeletal X-rays if the missing person has no next-of-kin, or if none can be located.
- If the missing person is still missing after 30 days, the release form (BICA 4048) must immediately be executed to obtain dental/skeletal X-rays and a photograph. The agency should confer with the coroner or medical examiner. The report, photograph, and dental/skeletal X-rays may be submitted to DOJ within 24 hours.
- If the agency determines the missing person may be "at risk," dental/skeletal X-rays and a recent photograph should be immediately obtained. The agency should confer with the coroner or medical examiner. The report and the dental/skeletal X-rays, including a signed DOJ Release Form (BCIA 4048), should be submitted to DOJ within 24 hours.
- If the missing person is still missing after 30 days, the reporting individual is required to obtain the dental records and give them, within ten days, to the law enforcement agency which took the initial report.
- If a missing person is found, a law enforcement agency must report this fact to DOJ within 24 hours.

DOJ forms can be located on CLEW.

Transmitting Reports to Other Jurisdictions
In cases where a report is initially taken by an agency that is not the agency of jurisdiction over the missing person's residence, the law enforcement agency taking the initial report must notify and forward without delay a copy of the report to that agency having jurisdiction over the missing person's residence and where the missing person was last seen. In cases involving children or persons at risk, this cross-reporting must be accomplished within 24 hours of initial receipt of the report.

A Reference Chart for MUPS can be viewed on CLEW. For additional information, refer to the POST *Missing Persons Investigations, Guidelines & Curriculum publication*.

Resources 3.14 - Photographs

Create or amend a written directive establishing procedures for processing, storing, and distributing photographs to include, at a minimum, the following:

- *Inmate photographs (e.g., booking photos, mug shots)*
- *Crime scene photographs*
- *Registrant and applicant photographs*

- *Accident photographs*
- *Photograph copies*

COMMENTARY
Records may be required to process, store, and distribute numerous photographs (e.g., agency personnel, registrants, applicants, booking photos, and crime scene images).

Inmate Photographs
Inmate photographs (e.g., booking photographs, mug shots), whether hard-copy or digital, are considered confidential records pursuant to PC 13300. Other photographs may be protected from release as well.

Crime Scene Photographs
Detailed procedures for photographing crime scenes are beyond the scope of this manual. Crime scene photographs should be considered and maintained as evidence in most cases. Refer to the POST *Law Enforcement Evidence & Property Management Guide* for information on the retention of evidence.

Registrant and Applicant Photographs
Sex and arson registrant photographs must be forwarded to DOJ with required documents.

Other applicant photographs are frequently required for specialized city and county licenses and permits. These photographs should be attached to the original report or related documents and filed in the appropriate location (e.g., registrant or applicant file).

Accident Photographs
Most agencies have some type of digital system to store accident photos. Accident photos should be printed only upon request and following payment of fees (if applicable). Accident photos must be retained in accordance with the agency record retention schedule. The release of photos depicting the body or any portion of the body of a deceased person may be restricted under CP 129.

Copies
A fee schedule should be established for reproducing photographs, whether digital or film based. Tracking documentation should ultimately be kept with the original case report in the master case file.

Resources 3.15 – Property
Create or amend a written directive establishing procedures for the processing of property-related documents by records personnel to include, at a minimum, the following:

- *Serialized property*
- *Property disposition*

COMMENTARY
The proper storage, safekeeping, and disposal of evidence and property require the cooperation of the records and property units. This commentary discusses those functions which are most often dependent upon records unit operations. Refer to the POST *Law Enforcement Evidence & Property Management Guide* for detailed guidelines on the law enforcement evidence/property function.

Property Reports
All property taken into custody must immediately be properly accounted for on an appropriate property receipt. A copy of the property receipt must be forwarded to records for inclusion in the case file. CC 2080.10
Receipt requirements pursuant to PC 1412, 1413, 1535, 18250, WI 8102 and 8103

Serialized Property
Law enforcement agencies must enter descriptions of serialized property including property with an owner applied number (OAN) which has been reported stolen, lost, found, recovered, or under observation, into the appropriate DOJ database according to PC 11108. Instructions are listed in the *CJIS Manual*, available on CLEW. The *Article/Brand and Category User's Guide* is also available on CLEW.

Property Disposition
Evidence and property are responsible for the control, release, and disposal of evidence and property. DOJ Notice of Arrest and Court Action form JUS 8715 is the most common means of notifying an agency when prosecution is concluded, and evidence is eligible for release or disposal. Records typically receives the form. The form must be filed with the report and the investigations or property unit notified to begin the disposition process.

Resources 3.16 – Record Sealing

Create or amend a written directive establishing procedures for the sealing of adult and juvenile records to include, at a minimum, the following:

- *Compliance with legal mandates*
- *Storage*
- *Destruction*

COMMENTARY
The court has the authority to seal arrest records under specific conditions. Records is responsible for processing requests to seal records. This section will discuss records sealing involving juveniles and adults.

Record sealing is a process designed to remove all references to an individual from agency files. Generally, the process is incident-specific (e.g., the records and references to a specific incident or arrest are sealed). Multiple records for one subject, unrelated to the court order, are usually unaffected by the sealing. In the case of

juvenile records, however, the court may order the entire record and reference to the juvenile sealed.

Upon receiving a court order to seal a record, appropriate notification must be made to every division within the agency to ensure all records pertaining to that subject are appropriately sealed. Additionally, notification of sealing must be made to anyone who has received a copy of the listed record and request the record be sealed, returned, or destroyed.

Record sealing is the collection of permanent records in a "package" ordered sealed by the court. This may be accomplished by removing specific references to the individual. Sealed records that must be held for destruction should be segregated from other records, and the petitioner's name and the date of destruction written on the envelope.

Legal Mandates
Sealing of records is mandated under certain conditions including the following: PC 851.6, 851.7, 851.8, 851.87, 851.91, 851.92 and WI 389, 781, 781.5, 786.

Juveniles
WI 389 (dependent child of the court) permits the involved person or a probation officer to petition the court to seal a record five years or more after the jurisdiction of the juvenile court has terminated as to the person; or in a case in which no petition was filed, five years or more after the juvenile was cited to appear before the probation officer or cited by the law enforcement agency or; in any case, at any time after the person has reached the age of 18. The court notifies the prosecuting attorney and the county probation officer who may testify why a record should not be sealed. If the sealing is granted, the court shall order the agency to seal its record and state the date to destroy the sealed record. Thereafter, only the court may inspect the sealed record or allow the record to be inspected. Additionally, the proceedings in the case are deemed not to have occurred. Any other agency in possession of sealed records shall destroy their records five years after the records were ordered sealed or as stated in the court order.

According to WI 781 (ward of the court), the involved person or a probation officer may petition the court to seal a record five years or more after the jurisdiction of the juvenile court has terminated as to the person; or in a case in which no petition was filed, five years or more after the juvenile was cited to appear before the probation officer or cited by the law enforcement agency or; in any case, at any time after the person has reached the age of 18. The court notifies the prosecuting attorney and the county probation officer who may testify why a record should not be sealed. If the court finds that the person has not been convicted of a felony or any misdemeanor involving moral turpitude and that rehabilitation has been attained, it shall order all records, papers, and exhibits in the person's case in the custody of the juvenile court sealed, and any other records relating to the case in the custody of the other agencies, entities, and officials as are named in the order. Once the court has ordered the person's records sealed, the proceedings in the case shall be deemed never to have occurred. If the sealing is

granted, the court shall order the agency to seal its record and state the date to destroy the sealed record. Thereafter, only the court may inspect the sealed record or allow the record to be inspected.

WI 781.5 Juvenile Factual Innocence permits a minor who has been cited to appear or has been taken before a probation officer, or a law enforcement agency, and no accusatory pleading has been filed, to request in writing that the jurisdiction over the offense find them factually innocent (no probable cause exists to believe that the offense was committed) and destroy their records of the arrest or citation. Upon a determination that the minor is factually innocent, the agency shall, with the concurrence of the prosecuting attorney, seal their records with respect to the minor and the request for relief under this section for three years from the date of the arrest or citation and thereafter destroy the records and the request.

In any case, where the request of a minor to the law enforcement agency, probation office, prosecuting attorney/district attorney and DOJ (LEA/PO/DA/DOJ) to have a record sealed and destroyed is denied, petition may be made to the juvenile court having jurisdiction over the matter. If the court finds the minor to be factually innocent, then the court shall order the LEA/PO/DA/DOJ and any agency that participated in the arrest or citation of the minor to seal their records relating to the minor and the court order to seal and destroy those records, for three years from the date of the arrest or citation and thereafter to destroy those records and the court order to seal and destroy those records. The court shall also order the LEA/PO/DA/DOJ to request the destruction of any records of the arrest given to any agency, person or entity.

Documentation of arrest or citation records that are destroyed pursuant to this section that is contained in investigative police reports shall bear the notation “Exonerated” whenever reference is made to the minor.

WI 786 Juvenile Completion of Probation
When a juvenile satisfactorily completes a program on informal supervision or a term of probation, the court shall order sealed all records pertaining to the dismissed petition in the custody of the juvenile court, and in the custody of LEA/PO/DA/DOJ. The court shall send a copy of the order to each agency and official named in the order, direct the agency or official to seal its records, and specify a date by which the sealed records shall be destroyed. Each agency and official named in the order shall seal the records in its custody as directed by the order. Upon the court’s order of dismissal of the petition, the arrest and other proceedings in the case shall be deemed not to have occurred.
A record that has been ordered sealed by the court under this section may be accessed, inspected, or utilized only by the prosecuting attorney, the probation department, the court, or the person whose record has been sealed, upon their request and petition to the court to permit inspection of the records, child welfare agency of a county responsible for the supervision and placement, and by the DOJ.

WI 787 Limited access to certain sealed records
A record sealed pursuant to Section WI 781, 786, or 786.5 may be accessed by a law enforcement agency, probation department, court, the DOJ, or other state or local agency that has custody of the sealed record for the limited purpose of complying with data collection or data reporting requirements that are imposed by other provisions of law. However, no personally identifying information from a sealed record accessed under this subdivision may be released, disseminated, or published by or through an agency, department, court, or individual that has accessed or obtained information from the sealed record.

PC 851.7(a) allows any person who was arrested as a juvenile for a misdemeanor to petition the court to have a record sealed. The individual must have been:

- Released per PC 849(b)(1)
- Released with charges dismissed or discharged without conviction, or
- Acquitted

The records of arrest for the following offenses cannot be sealed under PC 851.7:

- Offenses for which registration is required under PC 290
- Offenses under Division 10 (commencing with H&S 11000)
- Offenses of the VC or any local vehicle ordinance relating to the operation, stopping, standing, or parking of a vehicle

NOTE: Additional guidance regarding the sealing of juvenile records may be sought from local courts.

Adults
PC 851.8 permits a person who has been arrested, but where no accusatory pleading has been filed, to petition the arresting agency to destroy the record of the arrest. The arresting agency, upon a determination the person arrested, is factually innocent and with the concurrence of the district attorney, shall seal the arrest records, including the petition, for a period of three years from the date of arrest and thereafter destroy the record of arrest and the notice of sealing. DOJ and any other agency participating in the arrest shall be notified to comply with the same procedure. Any agency receiving a copy of the arrest record shall be notified to destroy the record.

The prosecuting attorney is served by the petitioner with a copy of the petition to seal the records. If the law enforcement agency does not respond to the petition within 60 days, the petition is deemed to have been denied. The requestor may then petition the court of jurisdiction to decide the petition.

PC 851.8(c) permits a person who has been arrested and an accusation was filed, but there was no conviction, to petition the court for a finding of factual innocence. If the court determines factual innocence, it will order the record sealed.

The arrestee shall be notified in writing by the law enforcement agency of the sealing and destruction of the record. This notice may be accomplished by returning the approved or denied petition to the individual. If reference is made to the arrest in any

other report, the notation, “exonerated” shall be made on the arrestee’s name or the name shall be obliterated.

No records shall be destroyed under the above section if any arrestee has filed a Civil action against a peace officer or law enforcement agency, or if the agency of record has received a certified copy of the complaint until the Civil action has been resolved. Petitions may be filed up to two years from the date of the arrest, or filing of the accusatory pleading, whichever is later. Time restrictions on filing under this section may be waived upon a showing of good cause by the petitioner.

PC 851.87 Prefiling Diversion Record Sealing

Whenever a person is arrested and successfully completes a prefiling diversion program in lieu of filing an accusatory pleading, the person may petition the superior court to issue an order to seal the records pertaining to an arrest and the court may order those records sealed as described in PC 851.92. A copy of the petition shall be served on the law enforcement agency and the prosecuting attorney who may request a hearing within 60 days of receipt of the petition. If the order is made, the court shall give a copy of the order to the person and inform the person that they may thereafter state that they were not arrested for the charge.

The person shall be advised that the arrest shall be disclosed by the DOJ in response to any peace officer application request and that this section does not relieve the person of the obligation to disclose the arrest in response to any direct question contained in any questionnaire or application for a position as a peace officer.

The person shall be advised that an order to seal records pertaining to an arrest made pursuant to this section does not affect a criminal justice agency’s ability to access and use those sealed records and information regarding sealed arrests, as described in PC section 851.92.

PC 851.91 Matter of Right Record Sealing

A person whose arrest did not result in a conviction may petition the court to have the arrest and related records sealed, as a matter of right or in the interest of justice PC815.91(a). An arrest did not result in a conviction if any of the following are true:

- PC 851.91(1)(A) The statute of limitations has run on every offense upon which the arrest was based, and no accusatory pleading was filed based on the arrest.
- PC 851.91(1)(B) The prosecuting attorney filed an accusatory pleading based on the arrest, but, with respect to all charges,
- PC 851.91(1)(B)(i) No conviction occurred, the charge has been dismissed, and the charge may not be refiled,
- PC 851.91(1)(B)(ii) No conviction occurred and the arrestee has been acquitted of the charges, (iii) a conviction occurred, but has been vacated or reversed on appeal, all appellate remedies have been exhausted, and the charge may not be refiled.

A Petition to Seal an Arrest form (form CR-409) shall be filed in the court in which the accusatory pleading based on the arrest was filed or, if no accusatory pleading was filed, in a court with criminal jurisdiction in the city or county in which the arrest occurred, at least 15 days prior to the hearing on the petition, and be served, by copy, upon the prosecuting attorney of the city or county in which the arrest occurred and upon the law enforcement agency that made the arrest at least 15 days prior to the hearing on the petition. The petitioner has the initial burden of proof to show that they are entitled to have their arrest sealed as a matter of right or that sealing would serve the interests of justice. If the court finds that petitioner has satisfied their burden of proof, then the burden of proof shall shift to the respondent prosecuting attorney.

If the court grants a petition pursuant to this section, the court shall furnish a disposition report to the DOJ, pursuant to PC 13151, stating that relief was granted under this section, and issue a written ruling and order to the petitioner, the prosecuting attorney, and to the law enforcement agency that made the arrest that states the record of arrest has been sealed as to petitioner, the arrest is deemed not to have occurred and other conditions.

PC 851.92 – Issuance of Court Ordered Record Sealing
When the court issues an order to seal an arrest, the court shall provide copies of the order and a report on the disposition of the arrest to the person whose arrest was sealed and to the prosecuting attorney, to the law enforcement agency that made the arrest, to any other law enforcement agency that participated in the arrest, and to the law enforcement agency that administers the master local summary criminal history information that contains the arrest record for the sealed arrest. Within 30 days of issuing the order, the court shall furnish a disposition report to the DOJ indicating that relief has been ordered and providing the section of the PC under which that relief was granted and the date that relief was granted.

The arrest record shall include, directly next to or below the entry or entries regarding the sealed arrest, a note stating, “arrest sealed” and providing the date that the court issued the order, and the section pursuant to which the arrest was sealed. This note shall be included in all master copies of the arrest record, digital or otherwise.

The state summary criminal history information shall include, directly next to or below the entry or entries regarding the sealed arrest, a note stating, “arrest relief granted,” providing the date that the court issued the order and the section of the PC pursuant to which the relief was granted. This note shall be included in all master copies of the arrest record, digital or otherwise.

A police investigative report, and court records related to the sealed arrest shall, only as to the person whose arrest was sealed, be stamped “ARREST SEALED: DO NOT RELEASE OUTSIDE THE CRIMINAL JUSTICE SECTOR,” and shall note next to the stamp the date the arrest was sealed and the section pursuant to which the arrest was sealed. The responsible local law enforcement agency shall ensure that this note is

included in all master copies, digital or otherwise, of the police investigative report related to the arrest that was sealed.

PC 851.87 and 851.91 – Access to records sealed under Arrest records, police investigative reports, and court records that are sealed under this section shall not be disclosed to any person or entity except the person whose arrest was sealed or a criminal justice agency. Nothing shall prohibit disclosure of information between criminal history providers. Notwithstanding the sealing of an arrest, a criminal justice agency may continue, in the regular course of its duties, to access, furnish to other criminal justice agencies, and use, including, but not limited to, by discussing in open court and in unsealed court filings, sealed arrests, sealed arrest records, sealed police investigative reports, sealed court records, and information relating to sealed arrests, to the same extent that would have been permitted for a criminal justice agency if the arrest had not been sealed.

Forms and the DOJ *Records Sealing Manual* are available on CLEW.

Resources 3.17 – Registrant Files

Create or amend a written directive establishing procedures for processing registrant files to include, at a minimum, the following:

- *Sex offender registration*
- *Juvenile sex offender registration*
- *Arson offender registration*
- *Gang registrants*
- *Notice of registration requirement*

COMMENTARY

The Sex Offender Registration Act can be found in Sections PC 290.

In 2021, California transitioned from a lifetime-based sex offender registration system to a tier-based system. Three tiers of registration for adult sex offenders were established, based on specified criteria, for periods of 10 years (tier one), 20 years (tier two), and for life (tier three). Juvenile offenders will be required to register as a sex offender for one of two registration tiers, either five years (tier one), or 10 years (tier two), as specified. Tier statuses will be reflected in the California Sex and Arson Registry (CSAR). The DOJ may place a registrant in a "to be determined" category for up to 24 months pending tier determination.

At the end of their minimum registration period, registrants who meet certain requirements may obtain proof of current registration from their registering law enforcement agency, and petition the superior court or juvenile court, in their county of residence, for termination of their requirement to register as a sex offender in California. Petitions for termination will be served on both the registering law enforcement agency (LEA) and the LEA in the county of conviction. The registering LEA shall report to the court on whether the registrant meets the mandatory minimum registration requirements

for termination. Based on specified criteria, the court will either grant or deny petitions for termination and notify the DOJ.

The DOJ shall make information available to the public via the Megan's Law website.

Detailed sex offender registration requirement information is available at the state of California Attorney General, and CLEW's Websites. Registrant fingerprints are submitted to DOJ via the Live Scan system, photos are uploaded via CalPhoto and the information is entered into the California Sex and Arson Registry (CSAR). Refer to *Guidelines for Submitted Live Scan Sex and Arson Registration Procedures,* published by DOJ and available on CLEW, for full explanations of forms, information requirements, and procedures.

Sex Offender Registration
An offender must register if:

- Convicted of an attempt to commit any of the offenses listed in PC 290, or
- Determined by the court to be a mentally disordered sex offender, or
- Convicted in any other state, federal, military, or foreign court of any offense which, if committed or attempted in California, would have been punishable as one of the above offenses

The offender:

- Is required to register within five working days of coming into a law enforcement agency's jurisdiction, and
- Must notify the last (previous) registering agency within five working days when they move out of their jurisdiction, and
- If enrolled at a college or employed at a college, must register with the agency having jurisdiction over the campus

A sex offender must register for the tier level to which they have been assigned by the courts and DOJ. Sex offenders can only be relieved of this responsibility by obtaining a Certificate of Rehabilitation pursuant to PC 4852.01.

A court can require a person to register for the conviction of any offense if the court feels the crime was committed for sexual gratification or from sexual compulsion.

Juvenile Sex Offender Registration
A juvenile sex offender (adjudicated a ward of the court) must register if convicted of violation of the following:

- 209 Kidnapping with the intent to violate sexual assault laws
- PC 220 Assault to commit rape, sodomy, or oral copulation
- PC 243.4 Sexual batter
- PC 261(c) Rape
- PC 264.1 Forcible sex in concert with another
- PC 266(c) Induce intercourse/sex acts by false representation with intent to create fear

- PC 267 Abduction of a minor for prostitution
- PC 286(b)(1)(c)(d) Sodomy of a person under 18 years of age
- PC 288 Lewd and lascivious acts on a child under 14 years of age
- PC 288a(b)(1),(c),(d) Forced oral copulation
- PC 288.5 Continual sexual abuse of a child under 14 years of age
- PC 289(a) Forcible penetration with a foreign object
- PC 647.6 Annoying or molesting a child under 18 years

A juvenile is required to register for the tier level to which they have been assigned by the courts and DOJ, or until their record is sealed under WI 781.

If convicted out of state of a comparable crime, they must register pursuant to PC 290(d)(4) within five days of residency,

Any court can require a person to register for the conviction of any offense if the court felt the crime was committed for sexual gratification or from sexual compulsion.

Arson Offender Registration
PC 457.1 requires an arson offender to register with the agency in the jurisdiction in which the offender lives if the offender has been:

- PC 451 Convicted of a violation of arson
- PC 451(a) Arson with great bodily injury
- PC 451(b) Arson of an inhabited structure/property
- PC 451(c) Arson of a structure or forest land
- PC 451(d) Arson of property
- PC 451(e) Arson while in custody
  PC 453(a) and (b) Every person who possesses, manufactures, or disposes of any flammable, or combustible material or substance, or any incendiary device in an arrangement or preparation, with intent to willfully and maliciously use this material, substance, or device to set fire to or burn any structure, forest land, or property
- Convicted of an attempt to commit any of the above offenses

The offender is required to register within 14 days of residence or change of residence and remain registered for life if the arson registrant was convicted after 1994.

Juveniles register for ten years, until reaching age 25 or until the record is sealed pursuant to WI 781.

Registration is not required if the subject has been granted a Certificate of Rehabilitation pursuant to PC 4852.01.

Gang Registrants
PC 186.30 requires individuals convicted of offenses determined to be gang-related to register with the law enforcement agency in the jurisdiction in which the individual resides, within 10 days of release of custody or within 10 days of taking residence in any jurisdiction. Registration is required for offenders convicted in a criminal court or who have had a petition sustained in a juvenile court for an offense listed in PC 186.22, or for any crime the court finds is gang-related at the time of sentencing or disposition. Registration requirements shall terminate five years after the last imposition of a registration requirement pursuant to PC 186.30.

Pursuant to PC 186.32 registration shall include the following:

- The registrant shall appear at the law enforcement agency. Juveniles must be accompanied by a parent or guardian.
- The law enforcement agency shall serve the registrant (and the parent, if a juvenile) with a California Street Terrorism Enforcement and Prevention Act notification, which shall include, where applicable, that the registrant belongs to a gang whose members engage in or have engaged in a pattern of criminal gang activity as described in PC 186.22(e).
- A written statement, signed by the registrant, giving any information which may be required, shall be submitted to the law enforcement agency.
- Fingerprints and a current photograph of the registrant shall be submitted to the law enforcement agency.

Registrants must inform, in writing, the law enforcement agency with which they last registered of a change of address within 10 days. If the new address is located in another agency's jurisdiction, the registrant shall register with the new law enforcement agency, in writing, within 10 days.

There is no requirement in the PC for this local information to be sent to DOJ.

Notice of Registration Requirement
CLEW and the California Sex and Arson Registration (CSAR) Website contain forms used to notify the registrants of their duty to register as a sex or arson offender. Their fingerprint impression and signature are required in the appropriate area on the registration forms, depending on the conviction offense for which they are registering.

The notice of registration document should be given to the offender to read, understand, and sign prior to their being released from custody, whether from a state correctional facility, county jail, or from court on probation (PC 290(b) and 290(c)). The sentencing court is responsible for completing the form if the offender receives probation or is charged with a fine. This document is used in court when a person fails to register and it is, therefore, extremely important that it is filled out completely and correctly.

Note: The offender may not receive the form as prescribed above. When an offender brings this form, the law enforcement agency may assist with the completion of the process.

Resources 3.18 – Secondhand Dealer and Pawnbroker Licensing

Create or amend a written directive detailing procedures for processing secondhand dealer and pawnbroker licensing to include, at a minimum, the following:

- *Determining applicant business meets the definition of a secondhand dealer or a pawnbroker under BP 21626 and Financial Code (FIN) 21000*
- *Providing and accepting applications for a secondhand dealer or a pawnbroker license*
- *Fingerprinting the applicant(s)*
- *Ensuring the pawnbroker applicant files the appropriate financial statement and surety bond with the agency*
- *Collecting and forwarding to DOJ the appropriate application forms and fees*
- *Issuing or revoking a secondhand dealer license or pawnbroker license pursuant to BP 21642 or FIN 21301*
- *Maintaining the current license status of all secondhand dealers and pawnbrokers within their jurisdiction*
- *Filing and retention of documents*

COMMENTARY

City and county licensing agencies are delegated the responsibility to implement the state Secondhand Dealer and Pawnbroker (SHD/PB) licensing process into their local licensing program pursuant to BP 21641. Chiefs of police and county sheriffs are required to accept an application from any person, entity, or corporation desiring to be licensed as a secondhand dealer or pawnbroker within their jurisdiction. There may be the need on the part of the applicant to apply for a business license within the jurisdiction. This applies to first-time applicants and renewals. Applicable code sections are BP 21641, 21642, and FIN 21300, 21301.

Although police and sheriffs are statutorily obligated for the licensing of secondhand dealers and pawnbrokers, this varies from city to city and county to county. The records section of a law enforcement agency, the investigations section regulating these businesses, the police commission, the city licensing section, or any combination thereof may be involved in the licensing of secondhand dealers and pawnbrokers within a jurisdiction.

DOJ is no longer accepting pawn slips from agencies: DOJ Bulletin 20-08-CJIS – the California Pawn & Secondhand Dealer System (CAPPS) has all necessary resource links and forms.

It is strongly recommended the directive incorporate the basic requirements for processing SHD/PB found under the Secondhand Dealer/PB tab on the CLEW homepage.

CLEW contains helpful documents for download, including:

- Applications which can be completed online (pdf)

- Becoming a Secondhand Dealer or Pawnbroker Manual
- Attorney General Opinion N.04-1001, April 6, 2005 (pdf)
- Secondhand Dealer/Pawnbroker Licensing Fee

Resources 3.19 – Special Incident Reporting Forms for Bombs/Incendiary Devices/Explosives

Create or amend a written directive for reporting and retaining records reported to the Federal Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) to include, at a minimum, the following:

- *Reporting activity through the ATF Bomb Arson Tracking System*
- *Purging*

COMMENTARY

Law enforcement agencies responding to bomb/incendiary devices/explosives must report their activity through the ATF Bomb Arson Tracking System. This task is generally handled by bomb squads. To ensure records of this activity are purged on an appropriate basis, best practice dictate they be included on the agency's records retention schedule.

Resources 3.20 – Subpoenas

Create or amend a written directive for the acceptance of and compliance with subpoenas to include, at a minimum, the following:

- *Designation of the agency's custodian of records and designee*
- *Accepting service of a subpoena*
- *Compliance with a subpoena*
- *Collect appropriate fees*
- *Adherence to specific laws and procedures*
- *Training*

COMMENTARY

A subpoena is a time-sensitive request to produce documents, or a request to appear in court related to a Civil or criminal case. Compliance to a valid subpoena served upon the agency is mandatory and non-compliance with its terms may be subject to Civil or criminal penalties, such as fines, jail time, or both.

Pitchess Motions

A Pitchess Motion is a request made by a defendant in a criminal action for access to information in the personnel file of an arresting police officer. Though rare, Pitchess Motions can also be made in Civil actions. (Pitchess v. Superior Court, 11 Cal.3d 531).

The following code sections may be applicable to the Pitchess Motions process:

- EVC 1043 – 1046 details the process for filing and the necessary document requirements
- Government Code (GC) Section 3300-3313 Peace Officers Procedural Bill of Rights

- PC 832.7 defines peace officer and/or custodial officer reports
- PC 832.8 defines peace officer and/or custodial officer personnel files

Subpoena Duces Tecum
Subpoena Duces Tecum (SDT) is a business process for obtaining records. Subpoenas may be for criminal or Civil matters and be on different forms, such as a DMV Admin Per Se SDT, Workers Compensation SDT, or federal subpoena forms. Request for production of a witness in court, records, evidence, people, Civil or criminal, etc.
The following code sections are applicable to the Subpoena Duces Tecum process:

- Evidence Codes (EVC) pertaining to subpoenas:
  - EVC 1270 defining government as a business
  - EVC 1328 address service of subpoenas electronically, by fax and mail
  - EVC 1530-1532 defines official writings and recorded writing
  - EVC 1560-1563 defines regarding compliance with a subpoena and reasonable fees

- Code of Civil Procedure (CP) Sections 1985-1987 defining subpoena and affidavit
- CP 2020.10-2020.510 Civil discovery act-producing records
- GC 7920.000 et seq., known as the "California Public Records Act"
- GC 68093, 68097, and particularly 68096.1, dealing with witness fees

This directive should be reviewed by the agency's legal representative. It is recommended the designated custodian of records attend detailed training in this area.

Resources 3.21 – Restraining Orders
Create or amend a written directive establishing procedures for entry of restraining orders to include, at a minimum, the following:

- *Types of restraining orders*
- *Process for timely entries into CLETS*
- *Proof of service*
- *Maintenance of documents (hard copy or electronic)*

COMMENTARY
There are several types of restraining orders law enforcement agencies may acquire or, in the case of an emergency, may initiate. Law enforcement agencies must enter Emergency Protective Orders (EPOs) into the California Restraining and Protective Order System (CARPOS) via CLETS. Some agencies serve as repositories entering orders into CLETS for other jurisdictions, such as a sheriff's department or the court.
A written policy must contain a process for timely entries into CLETS for the original entry proof of service, and maintenance of documents contained in files or in a records management system, paying close attention to the dates of validity and names (FAM Code Section 6380[d][1]).

Resources

- The CJIS Manual, located on CLEW, contains information bulletins and directions for entering restraining order information into CARPOS
- POST has certified training on domestic violence/restraining orders. Refer to the POST Course Catalog for presentation information
- The California Courts Protective Order Registry (CPOR) contains scanned copies of orders issued throughout California
- The POST Law Enforcement Evidence & Property Management Guide contains information on the surrendering of firearms in compliance with certain restraining orders
- The most current version of all restraining orders is available on the California Courts Website

Resources 3.22 – Vehicles

Create or amend a written directive establishing the processing of incidents involving vehicles to include, at a minimum, the following:

- *Entry/update of the DOJ Stolen Vehicle System*
- *Notice of Stored Vehicles*
- *Collection of fees*
- *Vehicle releases*
- *Private property tows*
- *Stolen, embezzled, and recovered vehicles*
- *Training*

COMMENTARY

Local agencies have specific, detailed responsibilities to document vehicles which are stolen, embezzled, recovered, stored, impounded, towed, and abandoned. Local agencies are further responsible to notify the owner of the vehicle's status, notify other law enforcement agencies, and maintain the flow of information between the agency and places of storage. Finally, a local agency must input and update the statewide automated Stolen Vehicle System (SVS) in the CLETS database.

Agencies should identify personnel members responsible for the legal notices, follow-up paperwork, and system entries, modifications, and cancellations in SVS. Agencies should also identify personnel to respond to public inquiries and preparation of the vehicle release authorization.

Resources

- The *CJIS Manual* (containing a chapter relating to the SVS) and the *DMV Manual for CLETS* are located under the publications tab on CLEW.

- The following code sections are applicable to vehicles:

    - PC 11108 Sheriff and police agencies must enter serialized and uniquely inscribed property into the SVS of CLETS

- VC 14602.6(a)(1) Authorizes a vehicle to be impounded for 30 days
- VC 14607.6 Authorizes forfeiture of a vehicle deemed nuisances
- VC 22852 Notification of vehicle storage to registered owner
- VC 22853 Authorizes removal of an abandoned vehicle and entry into SVS
- VC 10500(a) Mandates the entry into SVS any vehicle reported lost, stolen, embezzled, and the removal of the vehicle from SVS when recovered

Resources 3.23 – Warrant Processing

Create or amend a written directive establishing the processing of warrants to include, at a minimum, the following:

- Receiving and recording all incoming warrants
- Identifying the location of each warrant
- Identifying the status of each warrant
- Guarding against the loss of any warrant
- Providing a record of the attempts to serve each warrant
- Showing the final disposition of each warrant
- Responding to Serna Motions
- Citing and releasing misdemeanor warrants
- Picking up and expediting prisoners (transportation)
- Returning served/recalled warrants back to court

COMMENTARY

Warrants are court documents. Law enforcement agencies should have a warrant policy containing an effective system to receive, process, index, and maintain the status of warrants in all law enforcement databases (e.g., CLETS/NCIC) as well as local automated warrant systems. It is strongly recommended the directive include the documentation of due diligence and clearly define roles and responsibilities regarding who has access to original warrants and how warrants are identified as active, served, and recalled. Training should be included, as well as a process for purging warrants.

Each law enforcement agency is different and may have varying degrees of automation or participate in a county-sponsored warrant repository; the directive should include these outside resources.

Resources

- *CJIS Manual*, located under the publications tab on CLEW (contains mandated requirements for warrant entry into CLETS via the Wanted Persons System (WPS) database and instructions for placing the warrant in (NCIC)
- California Criminal Justice Warrant Services Association (CCJWSA)
- PC 105 Motion to continue a criminal case (Serna v. Superior Court [1985] 40 Cal.3d 239)

4. Confidentiality and Release of Information

PURPOSE
All records have the potential to be accessed by the public; however, agencies are bound by legal requirements to maintain confidentiality under defined circumstances. This chapter provides guidance on the confidentiality and dissemination/release of information.

This chapter addresses:
4.1 Confidentiality of records
4.2 Access to and release of agency records
4.3 Information which must be released
4.4 Exemptions to the release of information
4.5 Public Records Act response timelines, refusals, and fees
4.6 Documenting information release
4.7 Collision reports release
4.8 Other information release
4.9 Consequences for the unauthorized access of information

Resources 4.1 – Confidentiality of Records
Create or amend a written directive defining the confidentiality of records in accordance with applicable law to include, at a minimum, the following:

- *Compliance with California Public Records Act (CPRA)*
- *Compliance with any local "Sunshine Ordinances"*
- *Exemptions*

COMMENTARY
The CPRA (GC 7920.00 – 7931.000) defines "public records" as "any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics." Based upon this definition, the report of crimes and incidents written in the daily course of business of a law enforcement agency are public records and subject to release under the Act, with certain exemptions (see Resources 4.4).

Resources 4.2 – Access to And Release of Agency Records
Create or amend a written directive addressing access and release of agency records to include, at a minimum, the following:

- *Authorized/responsible personnel*
- *Access, release, and dissemination procedures*

COMMENTARY
Records personnel have many types of records within their control. Access should be limited to specific, identified individuals for a variety of reasons. Personnel releasing information must have extensive knowledge of the law which governs records release in order to make proper release decisions. In addition, records which are released should be annotated to support later release decisions and to enable information to be retrieved if the record is subsequently ordered sealed. The agency's legal counsel should review the directive before it is enacted.

Resources 4.3 – Information Which Must Be Released
Create or amend a written directive identifying information which must be released to include, at a minimum, the following:

- *Calls for service*
- *Crime/incident reports*
- *Arrestee information*
- *Specified recordings (audio or video) of incidents*
- *Specified content of officer personnel files*

COMMENTARY
The CPRA requires specific information to be released unless the release would endanger the safety of a person or endanger the successful completion of an investigation. The categories of information which must be released are:

- Calls for Service (Released to general public)
    - Time, nature, and location of all complaints or requests for assistance
    - Time and nature of response
    - Date, time, and location of occurrence
    - Date and time of report
    - Victim's name and age (victims of specific abuse and sex crimes or their parents or guardians [if the victim is a minor] may request this information be withheld-See PC 293)
    - Factual circumstances surrounding the crime or incident
    - General description of any injuries, property, or weapons involved

- Arrestee Information (Released to general public)
    - Full name and occupation of every individual arrested by the agency
    - Date of birth and physical description (sex, height, weight, color of eyes and hair)
    - Date, time and location of arrest
    - Factual circumstances surrounding arrest
    - Date and time of booking
    - Amount of bail
    - All charges, including warrants and parole or probation holds
    - Location where arrestee is being held
    - Time and manner of release

- Crime Reports (released to crime victims)
  Crime reports shall be released to the victim of an incident or an authorized representative thereof; an insurance carrier against which a claim has been or might be made; and any person suffering bodily injury or property damage or loss as the result of the incident caused by arson, burglary, fire, explosion, larceny, robbery, vandalism, vehicle theft, or a crime as defined by subdivisions (b) and (c) of GC 7923 and Marsy's Law.
  - Names and addresses of victims, arrestees, and witnesses *EXCEPT* confidential informants. Victims of specific abuse and sex crimes or their parents or guardians (if the victim is a minor) may request this information be withheld.
  - Description of any property involved
  - Date, time, and location of incident
  - All diagrams
  - Statements of involved parties
  - Statements of all witnesses *EXCEPT* confidential informants

- Critical Incident Video/Audio Recordings (Released to general public)
  - A critical incident is defined as: GC 7923.625(e)
    - An incident involving discharge of a firearm at a person by a peace or custodial officer.
    - An incident involving use of force by a peace or custodial officer against a person resulting in death or great bodily injury.
  - Several release limitations exist related to open criminal and/or administrative investigations, and rights of privacy of involved parties. Consult agency counsel when considering a release of these types of records.

- Disclosure of information required by law enforcement (Marsy's Law)

Law enforcement agencies are required to comply with several laws which either permit or require them to refuse to disclose information in their files. California Constitution, Article I, Section 28(b) (Marsy's Law) requires law enforcement agencies to provide copies of some of the otherwise protected documents to the State Board of Control or its designated local witness centers, upon request. Compliance with this section facilitates the operation of the Victims of Crime Act, which provides reimbursement to crime victims who incur expenses as a result of crimes which result in physical injury, and sex crimes resulting in either physical or mental injury. The records provided under California Constitution, Article I, Section 28(b) (Marsy's Law) are only released in order to submit and determine a claim under the Victims of Crime Act. Any further dissemination of the information is a misdemeanor.

Documents to be released by law enforcement agencies include:
- Complete copies of the original report
- Supplemental reports regarding the incident
- The petition filed in a juvenile court proceeding

The law enforcement agency may withhold the names of witnesses and informants if the release of the names would be detrimental to the parties or to an investigation currently in progress.

Resources 4.4 – Exemptions to The Release of Information

Create or amend a written directive identifying exemptions to the release and dissemination of information to include, at a minimum, the following:

- *Compliance with applicable laws and regulations*
- *Selective disclosures*

COMMENTARY

In order to balance the individual's right to privacy with the public's need for information, certain exemptions to the release of information are specified in GC 7923.600 or interpreted by court decision. These exemptions include:

1. Withholding disclosure of names, addresses, and identifying information of juveniles (under 18 years of age) – *Wescott v. Yuba County* (104 CAL APP 3d 103) and *T.N.G. v. San Francisco Superior Court* (4 Cal. 3d 767)(T.N.G. are the initials of the juvenile involved in this court decision)
   NOTE: It is recommended the definition of juvenile be verified with the juvenile court of the county. The exemption to release of information may pertain to all juveniles or only juveniles arrested, detained, or listed as suspects. Under *Wescott v. Yuba County*, the determination of the Appellate Court is all juveniles are under the protection of this decision. Therefore, all identifying juvenile information contained in a report is available for public release only if the County's T.N.G order authorizes such release. The presiding juvenile court judge issues the county's T.N.G. Order.
2. Confidential informants – GC 7923.605(a)
3. Criminal offender record information (CORI) – *Younger v. Berkeley City Council* (1975); PC 13300 and PC 11105
   NOTE: Release of CORI is based on an individual's right to know and need to know. The directive should define state and local CORI and the uses of CORI.
4. Information which may endanger the safety of a witness or other person involved in the investigation – GC 7923.605(a)(1)
5. Information which may jeopardize an investigation, related investigation, or law enforcement proceedings – GC 7923.605(a)(2)
6. Any portion of a report which reflects the analysis, recommendation, or conclusion of the investigating officer – GC 7923.603(b)
7. Confidential information provided only by a confidential source – *South Coast Newspapers, Inc. v. City of Oceanside* (1984)
8. Information which may disclose investigative techniques and/or procedures – *South Coast Newspapers, Inc. v. City of Oceanside* (1984)
9. Information which may deprive a person of a fair trial – *South Coast Newspapers, Inc. v. City of Oceanside* (1984)
10. Preliminary drafts, notes or memoranda which are not retained in the ordinary course of business – GC 7927.500

11. Records pertaining to pending litigation to which the public agency is a party until litigation is adjudicated or otherwise settled – GC 7927.200(a)
12. Personnel, medical, or similar files, the disclosure of which would constitute an unwarranted invasion of privacy – GC 7927.700 The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Adult victims of any crime defined by the following:

- PC 220 Assault to commit rape, sodomy, or oral copulation
- PC 261 Rape
- PC 262 Spousal Rape
- PC 264 Rape of a child under 14 years of age
- PC 264.1 Rape in concert with another
- PC 273a Child endangerment
- PC 273d Willful cruelty to a child
- PC 273.5 Assault on a spouse, co-parent, roommate, or former dating relationship
- PC 286 Sodomy
- PC 288 Lewd and lascivious acts on a child under 14 years of age
- PC 288a Oral copulation with a minor
- PC 289 Forcible sexual penetration with a foreign object
- PC 422.6 Hate Crime – interfering with another's constitutional rights
- PC 422.7 Hate crime – misdemeanor enhancement
- PC 422.75 Hate crime – felony enhancement
- PC 646.9 Stalking

Adult victims of any crime or their parents or legal guardians (if the victim is a minor), may request their names be withheld in addition to address and identifying data per GC 7923.615(b)(1). Pursuant to PC 293 and 293.5, the officer must document that confidentiality was offered to the victim, and the victim's response.

No law enforcement officer or employee of a law enforcement agency shall disclose to any arrested person, or to any person who may be a defendant in a criminal action, the address or telephone number of any person who is a victim or witness in the alleged offense (PC 841.5). The defendant may obtain necessary information through the discovery process. (This section does not affect the release of information contained in an accident report.)

The CPRA does not prevent a law enforcement agency from opening its records concerning the administration of the agency to public inspection unless disclosure is otherwise prohibited by law.

The attorney for a client may obtain the address and telephone number of victims and witnesses where the client may be a defendant in a criminal action in the alleged offense.

Selective Disclosures Prohibited
Once information is released to a member of the public, it becomes a public record and cannot be withheld from the public or the news media (*Black Panther Party v. Kehoe* (1974).

GC 7921.505(c)(5) allows the release of an exempt public record to any governmental agency which agrees to treat the disclosed material as confidential.

Resources 4.5 – Public Records Act Response Timelines, Refusals, and Fees

Create or amend a written directive addressing compliance with the CPRA to include, at a minimum, the following:

- *Public Records Act timelines*
- *Refusal to release information*
- *Fees*

COMMENTARY

Response Timelines
GC 7922.535(a) Outlines the timeliness of response to a request for records. Upon receiving a request, the public agency must determine within 10 calendar days whether or not the information will be provided. Notice of the decision must be made to the person requesting the record within the time limit. If "unusual circumstances," as defined in GC 7922.535(c), exist, an extension of not more than 14 calendar days is allowed to complete the determination.

Refusals
A law enforcement agency may refuse to release information per GC 7922.000.

Fees
GC 7922.530(a) permits a public agency to charge a fee to cover the direct costs of duplication of copies of non-exempted information, or a statutory fee if applicable.

Resources 4.6 – Documenting Information Release

Create or amend a written directive establishing procedures for the tracking of released information to include, at a minimum, the following:

- *Identifying released information*
- *Identifying recipient of information*

COMMENTARY
Whenever a report is released, a notation should be made on the report to identify to whom the document was released. If any information was redacted, a copy of the release should be saved by the agency to ensure no selective disclosure is made during future records requests. In the event an order is received to seal the record, the agency must be able to recall the document or request the receiving agency to destroy it.

Resources 4.7 – Collision Reports Release

Create or amend a written directive addressing the release of collision reports to include, at a minimum, the following:

- *Identifying information to be released*
- *Ensuring compliance with legal mandates*

COMMENTARY

VC 20012 requires the entire contents of a collision report to be released to involved parties or an authorized representative thereof; an insurance carrier against which a claim has been or might be made; and any person suffering bodily injury or property damage. This includes the original report, supplemental reports, diagrams, and photographs.

Resources 4.8 – Other Information Release

Create or amend a written directive addressing the release of miscellaneous information to include, at a minimum, the following:

- Activity logs: as defined by agency policy
- Personnel files: EVC 1043; GC 7927.700c; PC 832.7, 832.8, 13300(l-m); and Labor Code Section LAB 432.7(b)
- Background checks: Civil code Section CC 56; GC 1031.1; LAB 432.7 and 1198.5; Public Law 93-380; Title 5 USC 9101
- CLETS: CLETS Policy and Procedure Manual 1.4.7; GC 15153, 15163, 15165
- Licensing/permitting files: GC 7925.005
- Registrant files: PC 290, PC 457.1
- Citations: refer to Resources 3.4 - Citations
- Warrants: PC 168
- DMV files: VC 1808.45

COMMENTARY

Some jurisdictions have enacted ordinances requiring the broader disclosure of agency documents than those limited by the CPRA. Agency personnel should be familiar with agency mandates beyond legal requirements.

Resources 4.9 – Consequences for The Unauthorized Access of Information

Create or develop a written directive indicating the consequences for the unauthorized access of information and the unauthorized dissemination thereof to include, at a minimum, the following:

- *Legal sanctions*
- *Agency sanctions*

COMMENTARY

California law makes it a misdemeanor or felony to tamper or interfere with, damage, or illegally access a lawfully created computer data system. Access is defined as to gain entry, instruct, or communicate with the computer system or computer network.

Resources

- PC 502 Unlawful Dissemination of Information
- DOJ *CLETS Policy and Procedure Manual*

5. Statistical Reporting

PURPOSE
The purpose of this section is to introduce the elements and methods of statistical reporting as they apply to law enforcement activities. This chapter addresses:

5.1 Monthly Mandatory Reporting
5.2 Uniform Crime Reporting
5.3 Other Mandatory Statistical Reporting
5.4 Clery Act Reporting

Resources 5.1 – Monthly Mandatory Reporting
Create or amend a written directive requiring the identification and maintenance of records to provide statistical information as required by law to include, at a minimum, the following:

- *Compliance with legal mandates (PC 13020)*

COMMENTARY
Any statistical compilations and/or analyses produced are only as reliable as the information recorded in the original source document (often a crime or other report). Effective statistical reporting and analysis provide some valuable tools which can be used to impact crime, monitor program effectiveness, assist in decision making, and provide supporting data in other areas.

The following resources address specific reporting requirements. Refer to *Criminal Statistics Reporting Requirements*, published by the DOJ, for additional information.

Resources 5.2 – Uniform Crime Reporting
Create or amend a written directive establishing procedures for requiring the submission of and assigning agency personnel responsible for Uniform Crime Reports (UCR) to the FBI via the California DOJ to include, at a minimum, the following:

- *Summary Reporting System (SRS)*
- *National Incident Based Reporting System (NIBRS)* ***via*** *California Incident Based Reporting System (CIBRS)*
- *Hate Crime Statistics*

Data from the above three reports are collected and published by the FBI in a variety of publications including "Crime in the United States", and are also available via the FBI's "Crime Data Explorer" Website.

COMMENTARY

Due to the transitions between reporting systems, we have identified these sections as 5.2 A (SRS) and 5.2 B (NIBRS/CIBRS).

The FBI started the Uniform Crime Reporting (UCR) program back in the late 1920s to track crime nationally, discovering developing trends and to generate reliable information for use in law enforcement administration, operation, and management.

Over the years, the UCR data collected under the Summary Reporting System (SRS) has become one of the country's leading social indicators. Criminologists, sociologists, legislators, municipal planners, the media, insurance companies, publicly funded programs and other students of criminal justice use the data for varied research and planning purposes. However, the SRS data only told part of the story related to crimes in the United States.

Under the UCR program, the FBI collected summary information on ten crimes (eight in California) that either because of their serious nature, such as homicide, or their frequency, such as stolen vehicles, were likely to be reported to law enforcement. This system called Summary Reporting System (SRS) was in use up until early 2018 in most states, including California. Beginning in 2021, California joined the rest of the nation in using a more comprehensive approach to the tracking and reporting of crime statistics by utilizing the FBI's National Incident Based Reporting System (NIBRS). Because of additional reporting enhancements for California, the reporting system here is referred to as California Incident Based Reporting System (CIBRS).

Whereas the SRS was solely designed to track crime trends on only 8 crime categories, and only the most serious offense within an incident, NIBRS/CIBRS is intended to be much more of an analytical tool, tracking over 84 crimes and capturing all offenses and arrests occurring in an incident, not just one. Much more data about each incident and offense is gathered under NIBRS/CIBRS including information related to the offense, property, victim, offender, and arrestee. Benefits of the NIBRS/CIBRS system include:

- Distinctions can be made between attempted and completed crimes
- Detailed crime analyses can be made within and across LE jurisdictions
- Arrests and clearances can be linked to specific incidents and offenses
- Early detection of crime trends and forecasting crime occurrences
- Identify drug/alcohol/computer involvement with crime
- Assist research to enhance technology and the evaluation of record-keeping systems
- Greater focus and ID of victim, suspect and arrestee groups
- Assists in establishing Modus Operandi records
- Easy identification of weapons in crime

5.2 A - Summary Reporting System

Create or amend a written directive establishing procedures and assigning agency personnel responsible for requiring the submission of SRS statistics to the FBI via the California DOJ to include, at a minimum, the following:

- *By the 10th business day of each month, SRS includes the following federal and California reports:*
  - *Return a monthly return of offenses known to the police*

- *Supplements to return a:*
  - *Property stolen by classification*
  - *Property by type and value*
- *Supplementary Homicide Report*
- *Law Enforcement Officers Killed or Assaulted (LEOKA)*
- *Violent crimes committed against senior citizens*
- *Reports of domestic violence-related calls for assistance*
- *Arson offenses known to law enforcement*
- *Anti-reproductive rights crimes (ARRC)*
- *Monthly Arrest and Citation Register (MACR)*

Data from the above reports is collected and published by the FBI in a variety of publications including "Crime in the United States", and are also available via the FBI's "Crime Data Explorer" Website.

Part I crimes are offenses which most likely will be reported to law enforcement agencies based on their seriousness and frequency of occurrence. The eight crime classifications considered to be Part I offenses which must be calculated and reported to Criminal Justice Statistics Center (CJSC) by the 10th business day of each month for the previous month, listed by hierarchy, are:

1. Homicide
2. Rape
3. Robbery
4. Assault (simple & aggravated)
5. Burglary
6. Larceny (theft)
7. Motor vehicle theft
8. Arson

Based on the hierarchy rule, only the "highest" crime per incident is reported. The hierarchy rule is explained in detail in the *Summary Reporting System Handbook*. Reports can be submitted to the CJSC using:

- Hard-copy forms
- Electronic Crime and Arrest Reporting System (E-CARS) Software
- E-CARS Plus Web application

Hard-Copy Forms
Hard-copy forms are used to collect reportable data. The completed forms can be mailed or faxed to CJSC. Blank forms are available on CLEW or by contacting CJSC.

E-CARS Software
The E-CARS software provides agencies the ability to collect criminal justice statistics, ensure the data are complete and correct, maintain a statistical database, and generate monthly reports in an electronic media. Using the E-CARS software or record layout specifications, agencies can download the data onto a storage medium and mail their data to DOJ, or e-mail a file using the Pretty Good Privacy (PGP) encryption software.

E-CARS Plus Web Application
The E-CARS Plus Web Application provides California law enforcement agencies with an electronic means to collect, maintain, and report SRS statistics.
This application can be used by agencies with or without an RMS. For agencies utilizing an RMS, data in the proper format can be imported into E-CARS Plus. If an agency does not have an RMS, data can be entered directly into E-CARS Plus. No matter which method is used, when uploaded, the data is processed through validations to ensure it is complete and correct. Error resolution, revisions, and corrections to data are handled within this electronic environment. Users can run and print copies of submitted reports.
The full *E-CARS Plus Manual* is available on CLEW.

5.2 B – California Incident-Based Reporting System (CIBRS) and National Incident Based Reporting System (NIBRS) Crime Classifications

Create or amend a written directive establishing procedures and assigning agency personnel responsible for requiring the submission of NIBRS/CIBRS statistics to the FBI via the California DOJ to include, at a minimum, the following:
The NIBRS/CIBRS offenses are classified as group A and/or group B. They are additionally classified as either a crime against persons, a crime against property, or a crime against society.

COMMENTARY
NIBRS is capable of producing more precise and meaningful data because of the many facts about crime chronicled in the Group A Incident Report and Group B Arrest Report. Arranged in six topical segments (incidents, offenses, victims, known offenders and group A and B arrestees), elements describe various facts through specified data values that have been assigned data codes to condense the descriptions. The flexibility of this structure also permits NIBRS to adapt to keep up with modern crime issues.

Resources 5.3 – Other Mandatory Statistical Reporting

Create or amend a written directive establishing procedures and assigning agency personnel responsible for monthly reporting to the California DOJ to include, at a minimum, the following:

- *Death in custody report*
- *Juvenile detention report*
- *Racial Identity Profiling Act (RIPA)*
- *Use of force reporting (GC 12525.2)*
- *Crowd management reporting (PC 13652.1)*
- *Vehicle pursuits*
- *Law enforcement and criminal justice personnel survey*
- *Arrest dispositions*
- *Sex/arson registrants*
- *CLETS misuse (CLEW)*
- *Statewide Integrated Traffic Records System (SWITRS)*

- *Child abuse and child endangerment*
- *Elder abuse*
- *Missing persons*
- *California Values Act (GC 7284.6 (c)(1))*
- *U-Visa/T-Visa Persons applying for Visas may need sign off from a law enforcement agency (LEA) (PC 79.10(n))*
- *Complaints against law enforcement officers*

COMMENTARY

The death in custody report is required in any case in which a person dies while in the custody of a law enforcement agency or local/state correctional facility. Required to be filed within 10 days of the death and yearly.

The Juvenile detention report tracks data regarding the detention of minors.

The RIPA report requires annual reporting on all law enforcement stops as defined by RIPA.

Use of force reporting requires entry of all use of force instances involving serious bodily injury (GC 12525.2).

Crowd management deployment of kinetic energy projectiles and/or chemical agents requires monthly reporting on the department website of each instance.

Vehicle pursuits require reporting within 30 days to CHP on the CHP pursuit report form, each instance of a vehicle pursuit (VC 2800).

Law enforcement and criminal justice personnel survey requires annual reporting on the number of full and part time personnel.

Arrest disposition requires reporting within 30 days to DOJ the charges, agency, demographics, etc.

Sex and/or arson registrants requires reporting within 30 days to DOJ, via CSAR, all those who are mandated to register for sex and/or arson crimes.

CLETS misuse is reported each February 1st and accomplished a report on CLEW. SWITRS is provided to the CHP and includes completed traffic reports either electronically or hard copy by mail.

Child abuse/child endangerment is reported to DOJ on the for Suspected Child Abuse Report form (for mandated reporters) or Child Abuse or Severe Neglect indexing form (by child reporting agencies).

Suspected Child Abuse Report – Complete by mandated reporters.

Elder and/or dependent adult abuse is reported to DOJ for any reported crime on the for Report of Suspected Dependent Adult/Elder Abuse report form.

Missing persons reports are entered into the Missing and Unidentified Persons System (MUPS) per with varied time limitations as per the PC 14211(e).

Complaints against law enforcement officers should be reported on the Annual Report of citizens' Complaints Against Peace Officers, yearly to DOJ.

Most of these reporting requirements and forms are available on CLEW.

Resources 5.4 – Clery Act Reporting

NOTE: This resource applies only to colleges and universities participating in federal financial aid programs. These institutions may contact local law enforcement agencies for statistical data in order to comply with Clery Act reporting requirements.
Create or amend a written directive to ensure the agency complies with reporting provisions of the Clery Act.

COMMENTARY
The Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act (20 USC § 1092(f)) and 34 CFR 668.46 is federal law, originally known as the Campus Security Act, requiring colleges and universities to disclose information about crime on and around their campuses. The law is tied to an institution's participation in federal student financial aid programs and applies to most public and private institutions of higher education. The Act is enforced by the United States Department of Education.

The Clery Act requires colleges and universities to:

- Publish an Annual Security Report (ASR)
- Have a public crime log (institutions with a police or security department)
- Disclose crime statistics for incidents occurring on campus, in unobstructed public areas immediately adjacent to or running through the campus, and at certain non-campus facilities (including Greek housing and remote classrooms) to include:
    - Criminal homicide (murder & non-negligent manslaughter, negligent manslaughter)
    - Sex offenses (forcible, non-forcible)
    - Robbery
    - Aggravated assault
    - Burglary, where:
        - There is evidence of unlawful entry (trespass), which may be either forcible or not (unlawful entry must be of a structure having four walls, a roof, and a door)
        - There is evidence the entry was made in order to commit a felony or theft
    - Motor vehicle theft

    - Arson
    - The Violence Against Women Reauthorization Act (VAWA) of 2013 requires institutions to maintain statistics about the number of incidents of dating violence, domestic violence, sexual assaults, and stalking that meet the definitions of those terms
    - Requires institutions to report to the departments and disclose in the annual security reports the number of unfounded crime reports
    - Universities use the summary reporting system (SRS) for this reporting
- Report statistics for the following categories of arrests or referrals for campus disciplinary action (if an arrest was not made):
    - Liquor law violations
    - Drug law violations
    - Illegal weapons possession
- Ensure your policy assigns responsibility to issue Timely Warning Guide about Clery Act crimes which pose a serious or ongoing threat to students and employees
- Devise an emergency response, notification, and testing policy
- Compile and report fire data to the federal government and publish an annual fire safety report
- Enact policies and procedures to handle reports of missing students
- Report hate crimes by category of prejudice, including race, gender, gender identity, religion, sexual orientation, ethnicity, national origin, and disability; to include statistics for the following four crime categories if the crime committed is classified as a hate crime:
    - Larceny/theft
    - Simple assault
    - Intimidation
    - Destruction/damage/vandalism of property

6. Records Retention, Purging, And Destruction

PURPOSE
This chapter provides guidance on the retention, purging, and destruction of law enforcement records. It will provide the framework for a retention and destruction program. The retention of records required by law to be destroyed exposes agencies to potential Civil and/or criminal liability as well as potential damage to prosecution of cases. This chapter addresses:

6.1 Records Retention
6.2 Destruction Re `3 solution/Ordinance Preparation
6.3 Purge and Destruction of Records
6.4 Marijuana Records Destruction

Resources 6.1 – Records Retention
Create or amend a written directive defining records retention protocol and assigning agency personnel responsible to include, at a minimum, the following:

- *Complying with legal mandates*
- *Complying with agency or city/county policy (e.g., records retention schedule)*

COMMENTARY
The code sections listed below should be reviewed as they specify record retention periods.

Criminal Code Sections
PC 799, 800-806, 832 (Statute of Limitations)

Civil Matters
Part 2, Code of Civil Procedure (CP)

Gang Registrations
PC 186.20-186.33

Sex Registrations
PC 290

Alternative Storage Media
GC 34090.5 GC 12168.7 (City agency)
GC 26205 GC 12168.7 (County agency)
GC 14746 (State agency)

Resources 6.2 – Destruction Resolution/Ordinance Preparation
Create or amend a written directive establishing the framework and assigning agency personnel responsible for the preparation of a destruction resolution/ordinance to include, at a minimum, the following:

- *Considering the need for destruction*
- *Identifying specific records for destruction*

- *Identifying the method of record storage (electronic or hard copy)*
- *Complying with statute of limitations* (PC 799, 800-806, 832)
- *Requiring authorization of the agency head, city/county counsel, and governing body*

COMMENTARY
The following code sections present the framework within which a destruction resolution/ordinance must be prepared:

- GC 34090-34090.7 (City agency)
- GC 26205-26205.6 (County agency)
- GC 14745 and 14746 (State agency)

Resources 6.3 – Purge and Destruction of Records
Create or amend a written directive defining the process and assigning agency personnel responsible for the purge and destruction of records to include, at a minimum, the following:

- *Complying with legal mandates*
- *Identifying types of documents for purge/destruction*
- *Establishing date/method of purge/destruction*
- *Updating agency records/databases to reflect purge/destruction*

COMMENTARY
Purging is the identification and preparation of those records to be removed from active files for destruction or retention in another medium/location. The purging process involves the following:

- Verifying records retention schedule
- Reviewing documents by document type (e.g., crime report, citation, recordings)
- Determining storage method (electronic or hard-copy records)
- Determining disposition (e.g., destruction, movement to off-site location, or electronic storage)

The agency directive should consider the following documents to purge:

- Arrest reports
- Routine video monitoring, recorded radio, and telephone communications (GC 26202.6 - county and 34090.6 - city)
- Body-worn camera video (PC 832.18)
- Crime/incident reports and related materials (e.g., photographs)
- Collision reports
- Index cards/field interview cards
- Citations
- Correspondence
- Pawn slips
- Sex, arson, and drug registrations (PC 290)
- Licensing/permit files

- Repo, private property, storage, and impound files
- Citizen complaints/Pitchess documents
- Training files
- Personnel files
- Background files
- Other miscellaneous files maintained by the agency

If it has been determined the record is to be destroyed, a plan of action should be developed in compliance with the records destruction resolution/ordinance, to include:

- Destruction date by statute
- Method of destruction
- Update of appropriate databases
- Destruction/deletion of any copy of or reference to the destroyed record

Resources 6.4 – Marijuana Records Destruction

Create or amend a written directive outlining the procedures and assigning agency personnel responsible to ensure timely destruction of marijuana records in compliance with legal mandate to include, at a minimum, the following:

- *Adult records*
- *Juvenile records*

COMMENTARY

On November 9, 2016, the law related to marijuana offenses changed. Simple possession (less than an ounce) of marijuana for adults 21 years and older became legal. Also, for many people, possession of marijuana for sale, possession of marijuana for cultivation, and sales of marijuana became misdemeanors. H&S 11361.5(a) addresses marijuana records destruction. Agencies should contact their legal advisor for direction regarding the mandatory destruction of these records.

If a request is received for marijuana records destruction, interested parties can be referred to the Petition/Application (Form CR-400).

Exception: H&S 11357(e) juvenile records must be retained until the juvenile reaches 18 years of age.

Refer to the DOJ *Records Retention and Destruction Manual*, available on CLEW.

7. Automation of Records

PURPOSE
The purpose of this section is to provide an overview into automated records systems and resources for reviewing and evaluating current and future technology needs.

For a more detailed guide to successful management, planning, and implementation of any technology project, refer to the *Law Enforcement Tech Guide* published by the Office of Community Oriented Policing Services of the U.S. Department of Justice.

Almost all public safety and allied agencies have some type of an automated records management system (RMS), which usually interfaces with a computer-aided dispatch (CAD) system. RMS typically refers to a computer program (or set of programs) used to track and store records, although some agencies may still be on a paper-based system. Mobile data computers (MDC) linking local CAD and RMS systems to each other, as well as to state and local databases, are easing the workload of communications system operators and speeding the flow of information directly to the field officer. This chapter addresses:

7.1 Imaging
7.2 Live Scan/CAL-ID
7.3 Personnel, Training, and Capital Expenditure
7.4 Changes in Workflow and Procedures
7.5 Feasibility Study
7.6 Protection of Computer System Files & Resources

Resources 7.1 – Imaging
Create or amend a written directive establishing paper documents will be imaged, when possible, to integrate them into an RMS.

COMMENTARY
Document imaging is the process of converting paper documents to digital images, which are then securely stored on a cloud-based system, hard drive, CD, DVD, or other storage medium. Once information is entered into the imaging system, usually via a scanner, it is readily accessible for viewing or retrieval as needed and can eliminate the need for hard-copy paper distribution. Imaging can be designed to work with an existing RMS and/or CAD system. Imaging allows for safe, unalterable, and secure archiving of records. Reference GC 34090.5

Resources 7.2 – Live Scan/Cal-ID
Create or amend a written directive for the use of Live Scan technology to transmit fingerprint records to DOJ.

COMMENTARY
It is the intent of DOJ to require all fingerprints, applicant, or criminal, to be transmitted to them electronically. Electronic fingerprinting ensures accurate fingerprints are taken of the subject. This method of reporting greatly reduces the response time to positively

identify the subject, place the charges on the rap sheet, or to clear the prospective employee through a background process.

The California Identification System (CAL-ID) system is the automated system maintained by DOJ for retaining fingerprint files and identifying latent fingerprints. The CAL-ID system analyzes fingerprints and identifies crime perpetrators from the millions of records stored in its databases.

Resources 7.3 – Personnel, Training, And Capital Expenditure

Create or amend a written directive requiring assessment of personnel, training, and capital expenditure needs in relation to obtaining and maintaining an automated records system.

COMMENTARY

Implementing and maintaining an automated records system requires personnel trained in data entry, data quality control, system development and maintenance. It is critical to include records personnel in planning, implementation, or expansion of technology systems. Additionally, legal requirements must be met by these systems. (CLETS PPP) Records supervisors usually oversee document analysis, data entry, direct quality control efforts, coordinate computer support, and ensure compliance with state-mandated reporting requirements. More sophisticated systems typically require increased supervisory and management resources. Agencies may find it necessary to hire technology experts for managing information systems.

All users are required to be trained in the use of a new system. Training is the most important key to successful implementation of technology and automation. Resources and employee time should be allocated for system familiarization and start-up. Time should also be allocated for personnel to make periodic changes in formats, complying with new reporting requirements, and personnel refresher training. Initial system training as well as additional post-implementation training should be included as part of the performance agreement in the vendor contract negotiations.

Automating a records system requires a capital expenditure for hardware and software. Depending upon the size of an agency and the technology being purchased, the following factors should be considered during the planning stages:

- Major changes in workflow and procedures
- Licensing and ongoing maintenance fees
- Specific technical training for all personnel
- Increases in physical space requirements to accommodate multiple workstations with ergonomic considerations
- Temperature-controlled rooms housing computer servers
- New personnel with computer-specific technical skills

Resources 7.4 – Changes in Workflow and Procedures

Create or amend a written directive to address changes in workflow and procedures when acquiring new technology. The directive should, at a minimum, include the routine review of the following to maximize the benefits of new technology:

- *Policies*
- *Procedures*
- *Timetables*
- *Methods for processing documents and data*

COMMENTARY

When acquiring new technology, new policies and procedures should be written to effectively integrate the technology into the workplace and to safeguard the security of the information in the system.

Agencies depend on reliable, accurate, complete, and timely information. An automated system, alone, cannot correct all of the problems and deficiencies of a poorly designed records management process. The workflow should be examined, streamlined, and duplicate or unnecessary processes eliminated. The efficient retrieval, accuracy, and overall workflow of manual processes may be subtly enhanced through automation. A successful workflow automation will enable the agency and existing personnel to perform more efficiently.

When adding or changing technology which involves connection to national and state databases, agencies must conform to the FBI security policies and DOJ *CLETS Policies, Practices, and Procedures* (available on CLEW). This includes all computer systems (e.g., message switching computers, CAD systems, RMS systems) and local/wide-area networks connected directly or indirectly to CLETS. Contact CLETS Administration for detailed information and coordination.

Resources 7.5 – Feasibility Study

Create or amend a written directive requiring a feasibility study to be conducted when considering a major automation or technology project. The feasibility study process should include, at a minimum, the following:

- Form a feasibility study group and steering committee
- Develop a feasibility study plan
- Build support for the project
- Allocation of personnel including the selection of a systems analyst
- Define objectives of a desired information system
- Determine present system capabilities and resources
- Analyze needs
- Determine resource requirements
- Assess procurement options (if appropriate)
- Identify the desired system
- Prepare a report to the Steering Committee

COMMENTARY
Before proceeding with a feasibility study on automation, an audit of an agency's current system and business practices should be completed, and any deficiencies corrected. Some agencies assume, incorrectly, that automation is the only way to increase the accessibility, accuracy, productivity, and flow of information.

Steering Committee
To ensure executive personnel participation, a Steering Committee should be established to review and comment on the products prepared by the Feasibility Study Group (FSG). The Steering Committee should consist of high-level managers and/or supervisors from within the agency, appropriate to the project. This group will ensure a structured project management process is adopted and followed. The Steering Committee provides constant guidance and oversight to the project, its progress, and deliverables. Based upon the recommendations of the FSG, the Steering Committee will make most decisions related to the project and make final recommendations to the persons with the project purchasing authority.

Feasibility Study Group
An FSG, overseen by the project Steering Committee, should be established to determine what technology is needed and if the funding is available. It is very important this group include representatives of affected units and ranks within the agency. A typical study group for an RMS purchase may comprise the following:

- Chairperson (may be selected from group)
- Systems analyst(s)
- Sworn and Ccilian managers' representatives
- Sworn and Ccilian supervisors' representatives
- Patrol representative(s)
- Jail or corrections' representative(s)
- Property/Evidence representative(s)
- Investigation's representative(s)
- Records representative(s)
- Communications representative(s)
- Crime analyst representative(s)
- IT systems representative(s)
- Other stakeholders as identified by the agency

Group members should be chosen for their interest in the project, their knowledge of resources, user information needs, problem areas, and constraints.

Development of a Feasibility Study Plan
The FSG will define the study and develop a basic plan for carrying out the project. The plan should include:

- An outline of major steps to be followed in conducting the study
- A proposed time frame, including number of meetings planned per month
- A budget estimate of personnel costs and incidentals for the project

Building Support for the Study
Given the limited resources available for extensive studies and the potential cost of hardware and software, it is important to gain the early approval and cooperation of the city/county chief executive officer/administrator for the study project. Should the agency determine automation is an appropriate means to improve operations, the early support for the project ideas will prove beneficial to the agency. A two-pronged approach, using informal and formal lines of communication, should be considered to build support for the study.

Selection of a Systems Analyst
Once approval has been given to proceed with the feasibility study, a systems analyst should be selected.
The role of the systems analyst is to ensure a logical, comprehensive, and thorough plan is the basis for the needs analysis and system design. The analyst may be an agency employee, or an outside consultant chosen based on their ability to work with the FSG, communication skills, ability to generate ideas for system development, and knowledge of criminal justice records systems.
With preliminary planning for the feasibility study completed, the systems analyst and FSG should meet to assess, in concrete terms, the objectives of a good information system.

Determining Present System Capabilities and Resources
The FSG will determine the capability of the present system to deliver the type and quality of service desired. System capabilities can be determined by:

- Utilizing questionnaires and/or conducting interviews with all users
- Observing the system in use:
    - The flow of paper and/or information from input to output should be traced and documented in detail. This process will allow the systems analyst to identify each step in the process and the cost of each function. Documents should be evaluated as to their content and utility. This review often reveals opportunities for simplification, consolidation, or elimination of some data being collected.
- Identifying which existing functions could be replaced or modified/made more effective:
    - If implementation of a desired objective would eliminate all or part of an existing procedure, there will be an increase in system capabilities in proportion to the displaced service. For example, automating the UCR function eliminates the need for manual daily tallies and monthly recaps, and allows direct electronic transmission to state database terminals, thereby saving considerable clerical time, paper, and mailing costs. A report formerly taking six to eight hours to process by hand may take only five minutes with an automated system.
- Determining how existing resources can be better utilized, and what additional resources are required to attain the stated objectives
- Determining which resource (e.g., lack of personnel, lack of equipment, etc.) is the major constraint in attaining each of the stated objectives

- Identifying legal processes mandated for automated systems

Determining Resource Requirements
The FSG will determine the resources required to achieve the desired objectives. These resources may include operating personnel for the system, equipment, facilities, and supplies.

Specific costs for resources will generally fall into two categories: variable costs and fixed costs.

Variable Costs
- Personnel: The study should include an estimate of personnel requirements and related costs associated with operation of the system on a 24-hour basis, 7 day per week.
- Supervision: The need for supervision of both the system and personnel should be determined.
- Forms and Documents: The cost for each specific application and additional costs for new objectives or modifications to current procedures should be determined.
- Data Storage: Costs may include file cabinet space, computer and/or cloud storage, or an integrated document imaging system to maintain information online.

Fixed Costs
- Administration: Including management personnel time and related costs necessary to accomplish each objective. Included are the costs of specific operational personnel necessary for each task.
- Training: Including the cost of training personnel on new procedures, forms, software, and hardware. If training will be required for several new applications, the cost of personnel time and training may be divided among them. This cost should be considered when negotiating the purchase contract.
- Travel: Including the cost of off-site meetings and visits to other user agencies.
- Office Equipment and Supplies
- Hardware and Software
- Terminals and Lines: This includes costs for installation and purchase/lease of workstations, printers, and/or communication lines.
- Contractual Expenses: Contractual costs associated with the feasibility study include the following: software design, modification, annual maintenance, data migration and system transfer or forms design, which will occur as the direct result of the implementation of any objective.

Three important costing concepts should be considered when assessing resource requirements:
- Cost Avoidance: Occurs when a new application or system results in enhanced productivity or efficiency without an increase in current personnel or equipment.
- Cost Displacement: Occurs when a current expenditure for equipment, office

space, or personnel will no longer be required as a result of implementing a new program or application.
- Value Added: Defined as placement of a dollar value on less-tangible benefits typically associated with improvements in service delivery, crime analysis, forecasting, etc., which may occur as a result of a new application or system.

Determining System Objectives
The FSG will determine what tasks and processes the desired system will perform, and what benefits may be gained from its purchase.
Benefits may include:
- Increased productivity
- Decreased processing time
- Accelerated collection of fees (e.g., citations, bail, etc.)
- Space savings (paperless)
- Increased service to the public

Other consideration should be given to:
- Identifying all users of the agency's information system
- Cataloging user needs and the various ways information is utilized (crime analysis, statistics, research, etc.)
- Utilizing email
- Improving workflow
- Identifying reporting requirements; management, supervision, etc.
- Identifying system back-up requirements
- Identifying hardware and environmental requirements
- Integrating with legacy system or conversion of legacy system data
- Identifying external constraints on the system (privacy and security regulations, purging requirements, etc.)

This process should result in a list of desired outcomes the information system should provide.

Vendor qualifications should be defined and a list of references obtained. Site visits can be arranged with agencies utilizing the same system under consideration to discuss the pros and cons of the automated system with the end users. Financial assistance for such site visits may be available through the POST Field Management Training program. These site visits can be more informative than the vendor's sales presentation. It is important to review the types of problems an agency has encountered since installation of an automated system, and to discuss the vendor's responsiveness in resolving any technical difficulties.

Ranking Objectives
The FSG should rank the objectives in order of priority on the basis of the agency's needs. Needs can be grouped into four categories:
- Required: Federal, state, or local regulations require a new service or modification to an existing service or offer automated submission of required

reporting data.
- Critical: Inadequate procedures or lack of automation is a serious detriment to the efficient management of the department.
- Significant: Development of a new or modification of an existing application would produce significant improvement in the agency's functional capabilities.
- Desirable: The availability of automation or modification of an existing service would result in an improvement, but lack of implementation would not seriously affect the agency's overall operation.

Assessing Procurement Options
The FSG will determine which services or equipment should be procured and the estimated costs involved.

The following areas should be considered when evaluating a system which will automate a process:
- Capacity: Will the system be large enough to handle projected workloads and will the system allow for expansion?
- Access/performance: Will the system serve the number of users adequately and does it retrieve, or store documents as quickly as promised?
- Reliability: What components are likely to fail, how easily can they be replaced, and what will be the down time and the replacement costs?
- Support: Is there adequate after-sales support and prompt technical response available?

The acquisition of a computer system should begin with the identification of software systems meeting the needs of the agency. The most successful and efficient process identifies software first, and hardware second.

Custom-designed programs are costly and often have a longer start-up time and much higher cost than a packaged system. Maintenance of a custom system may run considerably higher because of the need to call technicians in to diagnose and repair system glitches or failures.

Once software has been identified as meeting the needs of the agency, it is appropriate to identify the hardware available to operate the software the agency may acquire. A consulting group can be of great assistance in determining the costs and advantages/disadvantages associated with acquiring a dedicated, shared, or leased system.

Reporting to Management
The FSG should prepare a complete report of the entire feasibility study for presentation to the Steering Committee who will review the presentation and make final recommendations to the agency administrator. The report should include:
- Scope of the feasibility study
- A discussion of the needs assessment process and results
- Advantages and disadvantages of alternatives recommended

- Cost/benefit analysis
- Recommendation of the best system

The agency administrator should decide whether to accept the recommendation and proceed with the acquisition and implementation of a new system. Due to the complexity of the issues and potential costs involved, an oral presentation by the systems analyst, in the presence of the FSG, to the Steering Committee is recommended. This process will allow questions to be asked, further information to be obtained and local/regional considerations to be reviewed.

Contract Negotiations
Agencies should follow their city/county/state procurement method when entering into contracts with vendors.

Often, a decision is made to accept open bids for the project, or in some cases a Request for Proposal (RFP) is extended for vendors to suggest the technology required to accomplish the automation. Regardless of the method used to attract vendors, the purchase of a new RMS will require negotiation of a detailed contract with the selected vendor.

Agencies should obtain every detail of the proposed project in writing. Considerations include:

- Vendor's responsibilities to manage the project
- Type of equipment to be installed
- Conformance with state and federal regulations or standards
- Background clearance through DOJ of selected vendor personnel
- Total cost of the installation
- Length of time to install the equipment
- Time required to convert hard-copy files and/or data files to the new system
- Set-up time to accomplish programming, testing, and debugging
- Security systems installed to protect sensitive data
- Conditions for acceptance of the equipment by the agency
- Ongoing technical service and maintenance
- Training provided for system administrators and users
- Term limit of upgrades and source code access
- Warranties on the equipment installed

An important component in a warranty agreement is to ensure the vendor has the ownership of the software installed. A thorough maintenance and training contract obtained from the vendor who installed the system will assure the agency has ongoing technical support and maintenance to keep the system operating at full capacity.

Resources 7.6 – Protecting Computer System Files & Resources

Create or amend a written directive to address protection of computer system files and resources. The directive should include, at a minimum, the following:

- *Back-up procedures for critical systems*
- *An alternate secure location to store back-up media off-site*

COMMENTARY

When transitioning from a manual system to an automated system, it is important to develop routine back-up procedures for RMS information. Automated systems can fail for a variety of reasons, including:

- Power outages
- Hardware or software failures
- Natural disasters, such as earthquakes, floods, or fires
- Intentional sabotage of the system caused by malware, network hacking or denial-of-service (DOS) attacks (by a disgruntled employee, terrorist or other)

Computer files should be backed up according to a regular schedule and comply with record retention laws or regulations. A regular check and/or update of passwords, access codes, and other security devices will maintain the integrity of the records system.

Back-up power generators should be tested and maintained on a regular basis (as often as possible). Power failure procedures should be in place and routinely exercised. Adequate fire detection and suppression equipment should be available. Temperature and humidity monitors should be in place and checked regularly.

While automation is the key to the future of law enforcement records management, a disaster recovery procedure should be established which can be put into operation and allow the agency to continue to operate when any of the above occurrences causes failure to the automated system (temporary or long-term).

8. Audits

PURPOSE
Audits are conducted to ensure compliance with applicable policies, procedures and legal mandates.

This chapter addresses:
8.1 External Audits
8.2 Internal Audits

Resources 8.1 – External Audits
Create or amend a written directive establishing procedures for complying with audits conducted by federal and state agencies in accordance with applicable laws to include, at a minimum, the following:

- *DOJ/CJIS audits*
- *FBI/NCIC audits*
- *DMV audits*

COMMENTARY
The audit concept of quality control is one of the standards set by the National Advisory Commission on Criminal Justice Standards and Goals (*Criminal Justice System*, Police Information Systems, Standard 4.7 - Quality Control of Crime Data).

In addition to the following requirements, 34 United States Code Section 10211 establishes a standard which is prescribed for records management and the establishment of maintenance standards for records.

DOJ/CJIS Audits and Monthly Validations
DOJ is required to audit each user agency to ensure compliance with CJIS and NCIC policies. Each agency, on a monthly basis, is required to validate entries made by the agency as being complete, accurate, and still active.

California Code of Regulations, Title II, Division 1, Chapter 7, Article 1, subsections 703(d) and 707(b) states the DOJ shall conduct audits of authorized persons or agencies using Criminal Offender Record Information (CORI) to ensure compliance with state regulations.

The Justice System Improvement Act (JSIA) regulations, 28 CFR, Section 20.1 et seq. address standards for the quality of criminal history record information. JSIA regulation 28 CFR, Section 20.21(a), subsection 5, requires criminal justice agencies to institute a process of data collection, entry, storage, and systematic audit which will minimize the possibility of recording and storing inaccurate information.

Note: DOJ and other regulatory agencies may audit various data bases within an agency for compliance with legal mandates (e.g., CalGangs, National Data Exchange

(N-DEx), etc.). These audits should be referred to the appropriate personnel within the agency.

FBI/NCIC Audits
The FBI is authorized to conduct security audits of any CJIS data in NCIC to ensure compliance with federal regulations. This is in addition to any California DOJ audit. Information for the above audits can be found on CLEW.

DMV Audits
Audit for confidentiality, insufficient information on source records, accuracy of justification for inquiries and/or misuse of system entries (DMV 9.000 VC 8057(b)). This includes Cal-Photo inquiries as well.(CLEW).

Resources 8.2 – Internal Audits

Create or amend a written directive establishing an internal audit process to include, at a minimum, the following:

- *Types of audits*
- *Who conducts audits and how often?*
- *Audit process*
- *Written reporting process*

COMMENTARY
The audit process involves the random sampling of reports, files, or procedures beginning at the origin of the event and tracking the process to final disposition. The reports or processes are closely inspected to ensure completeness, accuracy, and reliability. The internal audit process provides valuable information for improved performance. Each agency should determine the auditing configuration best suited to its needs.

Types of Audits
There are several types of audits. Those which impact the criminal justice field include:

- Management Audit: Examination and evaluation of an agency's organizational structure, plans, policies, and systems
- Operational Audit: Examination and evaluation of the efficiency and effectiveness of the use of resources and the extent to which practices and procedures adhere to policies established by management
- Compliance Audit: Examination to determine if certain legal requirements have been met

Who Conducts Audits and How Often
An agency should designate the person(s) responsible for conducting audits. The audit should be conducted by a mid-level manager or supervisor.
Although there are no set time frames for conducting audits, best practices dictate audits be planned and scheduled on a periodic basis, so all critical areas are covered within an established time period. Identified problem areas may require audits on a more frequent basis.

Audit Process
Several important areas of a law enforcement records system should receive routine audits/inspections. They include:

- Telephone/radio recordings
- Dispatch/complaint records
- Crime/incident reports
- Filing systems
- Data reporting
- Forms design/control
- Records dissemination
- Physical records security
- Data-entry procedures and security
- Department policy and manuals
- Financial records
- Personnel training
- Photocopying procedures
- Workplace communications
- Records retention
- Statistical record keeping
- Subpoena processes

The following questions should be considered when conducting the audit:

- Is there a valid need to perform the operation?
- Why is it performed?
- Why is it performed in a particular area?
- Why is it performed at a particular time?
- Why is it performed using a particular method?

Written Reporting Process
A report of the audit conclusions should be directed to the agency head with a copy provided to the Records Manager.

Glossary

Admin per se hearing (APS) - an administrative hearing that is conducted by a DMV hearing officer. An APS is different from a criminal proceeding. This process refers to the act of DMV suspending or revoking driving privileges.

Advanced Authentication - Provides for additional security to the typical user, identification and authentication of login ID and password. (CLEW)

Agency CLETS Coordinator (ACC) - Serves as the agency liaison to coordinate with Cal DOJ on matters pertaining to the use of CLETS, NCIC, NLETS, and the CA DOJ Criminal Justice Databases. (CLETS PPP)

Audit - A review or examination of records or processes for compliance with established policies and procedures. Audits are conducted to ensure compliance with applicable policies, procedures, and legal mandates.

Audit trail - the tracking of changes within an individual or group of records.

California Courts Protective Order Registry (CCPOR) - A statewide registry for storing data and images of restraining and protective orders.

California Incident-Based Reporting System (CIBRS) - California has a number of state-specific incident-based reporting requirements, including California specific data elements. These data points are in addition to the standard NIBRS data elements.

California Law Enforcement Telecommunications System (CLETS) - A restricted network that provides all law enforcement user agencies with the capability of obtaining information directly from federal, state and local computerized information files, for official use only.

California Law Enforcement Telecommunications System (CLETS) Administrative Section (CAS) - CLETS Administrative Section, the DOJ unit responsible for all CLETS administrative functions.

California Law Enforcement Telecommunications System (CLETS) IT Security Incident Form - the form used to notify DOJ when a computer incident (e.g., data breach, lost computer, hacking, etc.) occurs within your agency (see Computer Incident Response Plan). (Misuse Bulletin)

California Law Enforcement Website (CLEW) - A website maintained by the DOJ containing DOJ Bulletins, forms, manuals, and other information related to law enforcement criminal justice databases.

Cal-Photo - a DOJ repository that houses law enforcement agency booking photos, and the California Department of Motor Vehicles Driver License and Identification Card images.

California Restraining and Protective Order System (CARPOS) - A system used to upload protective order data through CLETS (formerly referred to as DVROS).

California Sex and Arson Registry (CSAR) - the state's mandated repository for sex and arson registration information and is used by law enforcement to register, manage, and track sex and arson registrants pursuant to California PC 290 and 457.1. (CLEW)

Certificate of Rehabilitation - Post-conviction relief in which a judge finds that a person has been rehabilitated following a criminal conviction. This process involves the individual filing a petition with the court (refer to PC 1203.4 and CLEW records sealing).

Commission on Accreditation for Law Enforcement Agencies, Inc. (CALEA) - A nationally recognized accreditation body for law enforcement agencies. The purpose of CALEA is to improve the delivery of public safety services by maintaining a body of professional standards that support the administration of accreditation programs.

Complaint - An accusatory pleading in a court of law charging an individual with a public offense.

Computer Incident Response Plan - a set of guidelines for how to respond and report a computer incident at a law enforcement agency. Examples of computer incident: stolen computer, virus/malware on computer, or suspected data compromise (See CLETS IT Security Incident Form CLEW).

Confidentiality - Refers to limitations on access to and use of information and documents that are protected by law or policy (the "right to know" and "need to know").

Court Order - A legal decision made by a court that commands or directs that something be done or not done. Can be made by a judge, commissioner, court referee, or magistrate.

Court Record - A written account of the proceedings in a case, including all pleadings, evidence, exhibits, and judgment submitted during the trial case.

Criminal Justice Data Exchange (CJDE) - A web-based application designed to improve how authorized agencies interact with the DOJ for criminal disposition processing and error retrieval. This application will facilitate improvement of criminal history information by providing a higher quality, timelier, and targeted information exchange between criminal justice agencies and the DOJ.

Criminal Offender Record Information (CORI) - Federal, state, and local records and data compiled by criminal justice agencies for purposes of identifying criminal offenders and of maintaining as to each such offender a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges, sentencing, incarceration, rehabilitation, and release.

Destruction Resolution/Ordinance - The process that identifies the types of records to be destroyed, approved by the governing body, with consent from the department head and the legal counsel of the city/county (Resources 6.2).

Detention Certificate - the document generated when an arrestee is released from custody as per PC 849. The arrest is deemed a detention and should be noted in all of the applicable records.

Discovery - The gathering of information (facts, documents, or testimony) before a case goes to trial. Discovery is done in many ways, such as through depositions, interrogatories, or requests for admissions. PC 1054 and CP 2017.010.

Dispositions - provides information about events, actions, and decisions taken or made by law enforcement, prosecutors, probation departments, courts, and the California Department of Corrections, subsequent to an arrest. The results of the dispositions contribute to the information on a subject's criminal history record.

Exemptions - Information that can be withheld from release to the public as defined by legal statute and court decision.

Forms Control - A system of centralized responsibility for the development, maintenance, numbering, revision, ordering, and supply of designated forms.

IT Security Incident Form (CLETS) - the form used to notify DOJ when a computer incident (e.g., data breach, lost computer, hacking, etc.) occurs within your agency (see Computer Incident Response Plan). (Misuse Bulletin)

Justice Automated Data Exchange (JADE) - A secure web-based user interface system which provides features for updating and querying the DOJ's Automated Criminal History System (ACHS). Information system available at California DOJ through JIM – see information Bulletin 18-15-CJIS.

Justice Identity Management System (JIMS) - used to provide account management services for CSARS, Cal-Photo, and other DOJ applications. JIMS will be utilized to add, modify, and deactivate users accounts.

Juvenile Court - That part of the superior court that handles delinquency, status offense, and dependency cases involving minors.

Juvenile Records - Those records pertaining to an individual under the age of 18 at the time of the incident.

Legal Hold - the temporary halt of alteration or destruction of records that may be relevant for litigation.

National Data Exchange (N-Dex) - Provides criminal justice agencies with a mechanism for sharing, searching, linking, and analyzing information across jurisdictional boundaries. This system is audited by the FBI on a triennial basis.

NexTEST - California DOJ CLETS testing program used to ensure compliance with Section 1.8.2 of the CLETS Policies Practices and Procedures (CLETS PPP).

Personnel Files - Employee's individual file that may contain any application, information, training records, memoranda, or internal investigation pertaining to an agency's present or past employees.

Petition - A formal written request given to the court asking for a specific judicial action.

Public Records - Any record containing information relating to the conduct of the public's business prepared, owned, used, or retained by any federal, state, or local agency, regardless of physical form or characteristics.

Racial and Identity Profiling Act (RIPA) of 2015 - AB 953 requires all city and county local law enforcement agencies in California, as well as the CHP and peace officers of California state and university educational institutions, to collect perceived demographic and other detailed data regarding stops.

Record of Arrest and Prosecution Sheet (RAPS) - Commonly used to describe the state of California criminal history record. (CLEW)

Retention schedule - a list of records series maintained by the organization that determines the length of time an item is kept and how it is destroyed.

Security Point of Contact (SPOC) (CLETS) – The person designated to serve as the security coordinator with the DOJ on security matters pertaining to the use of CLETS, NCIC, NLETS, DOJ criminal justice databases, and the administrative network the CLETS supports. (CLEW)

Statewide Integrated Traffic Records System (SWITRS) A California database that collects and processes data gathered from a collision scene.

Statute of limitations - The period during which legal action can be taken on Civil or criminal matters.

Subpoena Duces Tecum (SDT) - A type of subpoena that requires the witness to appear and/or produce a document or documents pertinent to a court proceeding. (Resources 3.20).

Terminal Access Request Form (TARF) CLETS - DOJ form, required for a new CLETS terminal(s), computer(s), or an access change to existing equipment. (CLEW)

T.N.G. Order – (Initials of juvenile involved in court case) - A court decision describing the methods for the release of juvenile information to a third party by a law enforcement agency. (WI 827)

Training for Trainers (T4T) CLETS - Refers to the Telecommunications Training for Trainers, a two-day class for law enforcement and criminal justice agencies to certify their trainers in the California Law Enforcement Telecommunications System (CLETS) and the National Crime Information Center (NCIC). T4T strictly refers to any and all train the trainer courses of instruction. (DOJ)

Uniform Crime Reporting (UCR) - Compilation of nationwide statistics submitted by law enforcement agencies throughout the country and available online. (No database reference)

URSUS - Use of force incident reporting, web-based data collection system, which allows law enforcement agencies to enter and submit use of force data to the DOJ.

Warrant - A written order issued and signed by a judge or judicial officer directing a peace officer to take specific action.

Web Resources

Accreditation	• Commission on Accreditation for Law Enforcement Agencies (CALEA), Inc.
Arrest and Dispositions	• CA Department of Justice, California Law Enforcement Web (CLEW) Arrest and Disposition Instruction Manual • Standards for Monthly Arrest and Citation Register (CA Department of Justice Dispositions) • User Manual Specifications and Juvenile Court and Probation Statistical System Reporting Standards • Electronic-Crime and Arrest Reporting System PLUS Electronic Crime and Arrests Reporting System Plus Manual
Attorney General Opinions	• Legal opinions of the Attorney General issued since 1986 may be viewed and searched on the DOJ Website • Printed volumes of Opinions of the Attorney General of California are published by Lexis Publishing and may be read in public libraries
Audits	• Assessing Completeness and Accuracy of Criminal History Record Systems: Audit Guide, U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics (January 1992, NCJ-133651 • The Role of Auditing in Public Sector Governance November 2006 (The Institute of Internal Auditors) www.theiia.org
Associations	• ANSI – American National Standards Institute • APCO International – The Association of Public Safety Communications Officials • ARMA – ARMA International • CCIAA – California Crime Intelligence and Analysts Association • CCJWSA – California Criminal Justice Warrant Services Association • CCUG California CLETS Users Group • CLEARS – California Law Enforcement Association of Record Supervisors • CPOA California Peace Officers Association • IALEP – International Association of Law Enforcement Planners • League of California Cities
Automation/ Technology	• Automated Information Sharing: Does It Help Law Enforcement Officers Work Better? (NIJ Journal No. 253 • January 2006) • Law Enforcement Tech Guide, U.S. Department of Justice, Office of Community Oriented Policing Services (2006) **Publications Available through the SEARCH Group, Inc., Website:** **Other Resources:** • A Guide for Applying Information Technology in Law Enforcement – National Law Enforcement and Corrections Technology Center *systems*-technology-enhancement-project

	• CA Secretary of State • Trustworthy Electronic Document or Record Preservation • AIIM ARP1-2009 Analysis, Selection, and Implementation of Electronic Document Management Systems • Law Enforcement Technology Needs Assessment • FBI Security Policy 5.9 (2020) • FBI Services
Citations	Judicial Council of California: • *Notice to Appear and Related Forms (2015),* • *Notice of Correction and Proof of Service,*
Criminal Statistics Reporting	*Criminal Statistics Reporting Requirements (2014),* California Department of Justice
DOJ Directory	Directory of Services – California Department of Justice (2022)
Fingerprinting / Registrants	• Guidelines for Submitting Applicant Live Scan Transactions • Guidelines for Agencies Receiving CORI • Guidelines for Submitting Criminal Live Scan Transactions • DOJ Applicant Fingerprint Clearance Manual CA Department of Justice, CLEW Client Services Program, Live Scan Support - Downloads and Manuals
Forms (State)	• California Department of Justice forms: California Law Enforcement Web (CLEW) • California Courts forms • California Department of Motor Vehicles forms: • CHP forms • California Firearms Laws, CA Department of Justice – Bureau of Firearms
Inmate Records	• California Department of Corrections and Rehabilitation, Title 15 • Board of State and Community Corrections • GC 7284 Cooperation with Immigration Authorities
Missing Persons	• POST Missing Persons Investigations, Guidelines & Curriculum
Periodicals	• *California Police Recorder*, California Law Enforcement Association of Records Supervisors, Inc., P.O. Box 3106, Lompoc, CA 93438 • *Information Management Magazine*, AMRA International, 11880 College Blvd., Suite 450, Overland Park, KS 66210 • *Law Enforcement Technology Magazine*, Officer.com, 1233 Janesville Ave., Fort Atkinson, WI 53538 • *Police 1: online resources for law enforcement* • *Peace Officer Research Association of California*
POST	The Commission on Peace Officer Standards and Training (POST) Website contains information on POST services and a host of other topics.

	• The POST Publications and Guidelines are an excellent resource for research assistance and information. • The POST Course Catalog contains a complete listing of all POST-approved courses. • POST Records Supervisor Certificate information can be found at http://www.post.ca.GC/records-supervisor-certificate.aspx.
Property	• *Professional Standards (2012),* International Association for Property and Evidence, Inc. • *Law Enforcement Evidence & Property Management Guide (2022,* California Commission on Peace Officer Standards and Training (POST) • *Law Enforcement Evidence & Property System Self-Assessment,* California Commission on Peace Officer Standards and Training (POST) • Assault Weapons Identification Guide
Public Records Act	• *The People's Business: A Guide to the California Public Records Act (2008)* • *First Amendment Coalition* • *GC 7920.000 California Public Records Act Eff Jan 1, 2023*
Records Management	• *Local Government Records Management Guidelines (2006),* California Secretary of State *Use and Management of Criminal History Record Information: A Comprehensive Report (2001 Update),* The National Consortium for Justice Information and Statistics (SEARCH) (NCJ 187670)
Records Security	• *Use and Management of Criminal History Record Information: A comprehensive Report (2001 Update),* U.S. Department of Justice, Bureau of Justice Statistics • California Law Enforcement Network (CLEW)
Registrants	• State of California, Attorney General's Office (Megan's Law): • California Law Enforcement Web • California Sex and Arson Registry (CSAR): Guide to Sex and Arson Registration Procedures:
Space Planning	*IACP Police Facility Planning Guidelines: A Desk Reference for Law Enforcement Executives (2019),* International Association of Chiefs of Police
Telecommunications	CA Department of Justice, California Law Enforcement Web (CLEW) • California Law Enforcement Telecommunications System Operating Manual • CJIS Manual • CLETS - Policies, Practices, Procedures (and statutes)
Training	**POST-Certified Records Training (See POST Course Catalog)** • Basic Records Course • Records Supervisor Course* • Public Records Act*

	*Successful completion of these courses is required to be eligible for award of a POST Records Supervisor Certificate **Additional records training is offered through:** • POST Learning Portal • California Crime and Intelligence Analysts Association • California Law Enforcement Association of Records Supervisors (CLEARS) • California CLETS Users Group (CCUG) • California Criminal Justice Warrant Services Association (CCJWSA) • California Division of the International Association for Identification (IAI) • Embassy Consulting • Law Enforcement Enterprise Portal (LEEP) • PRI Management Group
Vehicles	CA Department of Justice, California Law Enforcement Web (CLEW) • DMV Manual for CLETS • DMV Law Enforcement Resource Guide • DMV Information Search for Law Enforcement Only • DMV Bulletins and Publications Transactions

Legal Reference

For ease of use, legal references are depicted on the following pages in two ways:

- by Code/Section
- by Topic

Case law decisions are not included in the POST *Law Enforcement Records Management Guide* because of the fluidity of the law and the difficulty of maintaining current reference materials. POST recommends agencies refer legal interpretations and case law decision research to their legal counsel in order to obtain a current legal opinion.

CATEGORY TABLE
The following is an alphabetical reference of legal codes pertinent to the law enforcement records management. Agencies should confirm the accuracy and applicability of statutes within these codes when they are referenced within written policies. Use this list as a reference to abbreviations used for statutes cited within this Guide.

STATUTE	**Abbreviations used within this guide**	**ABBREVIATION per https://leginfo.legislature.ca.GC/faces/codes.xhtml**
Business and Professions Code	BP	BPC
Civil Code	CC	CIV
California Code of Regulations	CCR	CCR
Code of Civil Procedure	CP	CCP
Code of Federal Regulations	CFR	CFR
Education Code	EDC	EDC
Evidence Code	EVC	EVID
Family Code	FAC	FAM
Financial Code	FC	FIN
Government Code	GC	GOV
Health and Safety Code	HS	HSC
Labor Code	LAB	LAB
Penal Code	PC	PEN
United States Code	USC	USC
Vehicle Code	VC	VEH
Welfare and Institutions Code	WI	WIC

LEGAL REFERENCE
(By Code/Section)

CODE OF FEDERAL REGULATIONS
28 CFR 20.1 – *(Audits)* Justice System Improvement Act; need for CORI audits

UNITED STATES CODE
20 USC § 1092(f) – *(Campus Statistics)* Clery Act

CALIFORNIA CONSTITUTION
California Constitution, Article I, Section 28(b) (Marcy's Law) – *(Information Release)* Copies of protected documents to Board of Control

CALIFORNIA CODE OF REGULATIONS
California Code of Regulations, Title II, Division 1, Chapter 7, Article 1, subsections 703(d) and 707(b) – *(Audits)* Established requirement for DOJ audit of CORI dissemination

BUSINESS & PROFESSIONS CODE
BP 6054 – *(Information Release)* Cooperation; assistance with State Bar
BP 1625-28 – *(Licensing)* Secondhand dealer licensing requirements/reporting
BP 1634 – *(Reports)* Stolen non-serialized property report to DOJ
BP 4202 – *(Premise Violations)* Requirement to report arrest to ABC

CIVIL CODE
CC 798.32-.44 – *(Information Release)* Right of inquiry inspection of personal information
CC 798.53 – *(Information Release)* Intentional disclosure; Civil action

CODE OF CIVIL PROCEDURE
CP 28 – *(Subpoenas)* Powers of court; compliance with subpoena
CP 29 – *(Photographs)* Restricts release of photographs of deceased persons
CP 985-1987 – *(Subpoenas)* Defines subpoena and affidavit requirements
CP 002-2015 – *(Subpoenas)* Defines manner of production, mode of testimony, and affidavits offered as testimony
CP 2016-2036 – *(Subpoenas)* Discovery
CP 2020.10-2020.510 – *(Subpoenas)* Nonparty discovery
CP 2023 – *(Subpoenas)* Procedure for a subpoena regarding deposition of witness within this state in foreign actions
CP 2024 – *(Subpoenas)* Deposition of witness for an out-of-state witness in actions within this state

EDUCATION CODE
EDC 10911.5 – *(Records Check)* Public recreation employees; fingerprinting
EDC 35021.1 – *(Records Check)* Automated records check volunteer aids/sex offenses, conviction

EDC 35254 – *(Records Sealing/Destruction)* Destruction of school district records; microfilming
EDC 44237 – *(School Employees)* Bar from employment for sex/narcotics offenses
EDC 45123 – *(School Employees)* Bar from employment for sex/narcotics offenses
EDC 45124 – *(School Employees)* Bar from employment; sexual psychopath
EDC 45125 – *(School Employees, Records Check)* Requirement for fingerprints/state criminal history check
EDC 45126 – *(School Employees)* Duty of DOJ to furnish information
EDC 88022 – *(School Employees)* Bar from employment for sex/narcotics offenses; community colleges
EDC 88023 – *(School Employees)* Bar from employment; sexual psychopath; community colleges
EDC 88024 – *(School Employees, Records Check)* Requirements for fingerprints/state criminal history check; community colleges
EDC 88025 – *(School Employees)* Duty of DOJ to furnish information, community colleges

EVIDENCE CODE
EVC 250-260 – *(Information Release)* Definitions; writings; original; duplicate
EVC 1040 – *(Information Release)* Privilege/conditions for refusal to disclose information
EVC 1043 – *(Pitchess Motions)* Establishes guidelines for discovery/disclosure of peace officer records
EVC 1270 – *(Information Release)* Defines Government as business
EVC 1271 – *(Information Release)* Admissible writings and exceptions to hearsay rule
EVC 1506 – *(Information Release)* Copy of public writing
EVC 1507 – *(Information Release)* Copy of recorded writing
EVC 1508 – *(Information Release)* Other secondary evidence of writings
EVC 1509 – *(Information Release)* Voluminous writings
EVC 1530-1532 – *(Information Release)* Official writings
EVC 1560 – *(Subpoenas)* Compliance with subpoena duces tecum for business records
EVC 1561 – *(Subpoenas)* Affidavit accompanying records
EVC 1562 – *(Subpoenas)* Admissibility of affidavit and copy of records
EVC 1563 – *(Subpoenas)* Witness fees and mileage
EVC 1564 – *(Subpoenas)* Personal attendance of custodian and production of original records
EVC 1565 – *(Subpoenas)* Service of more than one subpoena duces tecum

FAMILY CODE
FAC 6345 – *(Restraining Orders)* Restraining order expiration dates

FINANCIAL CODE
FC 777.5 – *(Information Release)* Release of information to banks for employment
FC 6525 – *(Information Release)* Release of information to financial assistants for employment

FC 14409.2 – *(Information Release)* Release of information to credit unions for employment
FC 21208 – *(Reports)* Pawn/buy reports to DOJ

GOVERNMENT CODE
GC 6200-6203 – *(Information Release)* Penalty for theft, destruction, etc., of public records
7 GC 7920.200 – *(Information Release)* Effect of prior rights and proceedings
7 GC 7920.500-7920.545– *(Information Release)* Definitions under CPRA
7 GC 7921.000 – *(Information Release)* Public Records Act 2021 defines and regulates release of public records
7 GC 7922.000 – *(Information Release)* Justification for withholding of records
7922.525-7922.545 – *(Information Release)* Public records open to inspection; time; guidelines and regulations governing procedures
GC 7922.530 – *(Information Release)* Entitled to a copy
GC 7922.535 - *(Information Release)* Respond with 10-14 days (Former 5253(c))
GC 7922.600-7922.605 - (*Information Release)* Duty to assist
GC 7922.630-7922.640 – (*Information Release*) Regulations
GC 7923.000-7923.500 – *(Information Release)* Public recourse for failure to provide information requested, proceedings
GC 7923.630 – (*Information Release*) Law Enforcement record exemption and what must be disclosed from them
GC 7923.650 – *(Information Release)* Disclosure to prosecuting attorney
GC 7930.000-7930.005 – *(Information Release)* Exemptions to CPRA
GC 12525 – *(Reports)* Death-in-custody reporting
GC 13951 – *(Information Release)* Definitions (victim, injury, crime)
GC 14745-46 – *(Records Sealing/Destruction)* Destruction of state records; authority
GC 15150-67 – *(CLETS)* Establishes California Law Enforcement Telecommunications System
GC 26201-02 – *(Records Sealing/Destruction)* Destruction of county records; authority
GC 26205 – *(Records Sealing/Destruction)* Destruction of certain records; conditions
GC 27491 – *(Information Release)* Coroner's records
GC 34090-90.5 – *(Records Sealing/Destruction)* Destruction of city records; authority
GC 34090.6 – *(Records Sealing/Destruction)* Destruction of communication tapes; authority
GC 34090.7 – *(Records Sealing/Destruction)* Destruction of duplicate records less than two years old
GC 54985-87 – *(Information Release)* Fees
GC 68093-97 – *(Subpoenas)* Witness fees

HEALTH AND SAFETY CODE
HS 1522(a) – *(Information Release)* Access to CORI by Department of Social Services
HS 1522.06 – *(Information Release)* Providing CORI obtained by CLETS to a county child welfare agency
HS 11357(e) – *(Marijuana)* Juvenile possession on school grounds
HS 11361-61.5 – *(Marijuana)* Purge requirements

HS 11361.7 – *(Marijuana)* Accuracy, timeliness, and completeness of destruction; application
HS 11591-91.5 – *(School Employees)* Notice to school authorities; controlled substance offenses

LABOR CODE
LAB 432.7-432.8 – *(CORI)* Regulates disclosure for employment, penalties for violation
LAB 432.7(b) – *(CORI)* Arrest and detention of peace officer

PENAL CODE
PC 146(b) – *(Information Release)* Simulating official inquiries
PC 166.4 – (*Firearms, Restraining Order)* Violation of a court order
PC 168 – *(Information Release)* Release of felony warrants
PC 186.30 – *(Registrants)* Gang registrants
PC 273.6 – *(Firearms, Restraining Order)* Violation of domestic violence restraining order
PC 290 – *(Registrants)* Sex offender registration requirements
PC 291-291.5 – *(School Employees)* Notice to school authorities of arrest for sex crime
PC 293 – *(Information Release)* Victims of sex offenses may request that names not be disclosed
PC 457.1 – *(Registrants)* Arson offender registration requirements
PC 502 – *(Computer Systems, CLETS)* Theft from; malicious access/damage; penalties
PC 530.5 – *(Information Release)* Willful use of personal identifying information; records to reflect innocence of person whose identity was falsely used
PC 691 – *(Criminal Procedures)* Accusatory pleading defined
PC 799-805 – *(Statute of Limitations)* Statute of limitations; criminal
PC 806 – *(Criminal Procedures)* Examination before magistrate
PC 832.5 – *(Complaints)* Citizen complaints against agency personnel
PC 832.7-832.8 – *(Peace Officers)* Peace officer records; confidentiality
PC 841.5 – *(Information Release)* Confidentiality of victim and witness information
PC 849.5 – *(Detention Only, Reports)* Arrest deemed detention only, requirements
PC 851.6(a) – *(Detention Only)* Detention certificate requirements
PC 851.7 – *(Records Sealing/Destruction)* Petition to seal a record; minor
PC 851.8-851.85 – *(Records Sealing/Destruction)* Factual innocence; sealing/destruction requirements
PC 853.6(g) – *(Citations)* Citations; booking required on recordable offenses
PC 988 – *(Criminal Procedures)* Arraignment
PC 1054.5 – *(Subpoenas)* Criminal discovery
PC 1203 – *(Probation)* Authority to grant; conditions of probation
PC 1203.4 – *(Probation)* Discharged probationer; conviction set aside; reimbursement of county costs
PC 11075-81 – *(CORI)* Definition; dissemination; requirements to regulate dissemination
PC 11078 – *(CORI)* Requirement to maintain listing of agencies to whom CORI is released
PC 11105 – *(CORI)* Requirements/restrictions in furnishing state summary information

PC 11105.02 – *(CORI)* Screening on concessionaires; CORI provided to local government
PC 11105.03 – *(CORI)* Public housing authorities; access to information
PC 11105.3 – *(CORI)* Youth organizations and human resource agencies access to state CORI for employment/volunteers
PC 11105.4 – *(CORI)* Security organizations access to state and local CORI for employment

PC 11105.6 – *(CORI)* Bail bond agents access to CORI
PC 11107 – *(Reports)* Local reports required to be submitted to DOJ
PC 11108 – *(Property)* Requirement to submit reports of lost, found, or stolen property that is serialized
PC 11109 – *(Fingerprint Cards)* Coroner's records; decedent fingerprint cards required
PC 11115 – *(Dispositions)* Arrest and court action disposition requirements
PC 11120 – *(CORI)* Record defined
PC 11124 – *(CORI)* Determination of existence of record; copy of record or notice of no record; delivery
PC 11125 – *(CORI)* Prohibition from requiring subject to obtain copy of state record
PC 11126 – *(CORI)* Procedure for correction/clarification of state record
PC 11127 – *(CORI)* Requirements for DOJ to adopt regulations
PC 11140 – *(CORI)* Definition of state record
PC 11141-43 – *(CORI)* Penalties for unauthorized possession/dissemination of state summary records
PC 11144 – *(CORI)* Dissemination for statistical/research purposes; authorized and defined; state
PC 11166 – *(Child Abuse)* Reporting requirements
PC 11167 – *(Child Abuse)* Child abuse reports; disclosure
PC 11167.5 – *(Child Abuse)* Protects child abuse reports
PC 11169 – *(Child Abuse)* Written notification to suspect of report to child abuse central index
PC 12070-77 – (Licensing) Firearms dealers; dealer record of sale
PC 13020 – *(Reports)* Statistical reporting to Attorney General
PC 13022 – *(Reports)* Annual justifiable homicide reporting to DOJ
PC 13023 – *(Reports)* Hate crimes reporting to Attorney General
PC 13101 – *(Information Release)* A criminal justice agency@ defined
PC 13102 – *(CORI)* CORI definition
PC 13103 – *(Records Sealing/Destruction)* Destruction of original records; conditions
PC 13104 – *(Information Release)* Certified reproduction of any record
PC 13150 – *(Reports)* Reporting requirements to DOJ
PC 13151 – *(Dispositions)* Arrest and court action disposition requirements
PC 13202 – *(CORI)* Dissemination for statistical/research purposes; local CORI
PC 13300-01 – *(CORI)* Requirements/restrictions in furnishing local summary information
PC 13302-04 – *(CORI)* Penalties for unauthorized possession/dissemination of local summary records
PC 13305 – *(CORI)* Dissemination for statistical/research purposes; local CORI

PC 13320-23 – *(CORI)* Right to examine and challenge state record, fees, and procedures
PC 13324 – *(CORI)* Procedure for correction/clarification of local record
PC 13325 – *(CORI)* Requirement for local record review
PC 13326 – *(CORI)* Prohibition from requiring subject of record to obtain copy of local record
PC 13700-02 – *(Domestic Violence)* Domestic Violence Act
PC 14200-15 – *(Missing Persons)* Reporting requirements
PC 18250-18275 – *(Domestic Violence)* Take custody of weapons
PC 26185 – *(Firearms)* CCW Applications, fingerprints
PC 26500(a) – *(Licensing, firearms)* Firearms dealers; dealer record of sale

VEHICLE CODE
VC 28 – *(Vehicles)* Vehicle repossession notification
VC 808.45-1808.47 – *(Information Release)* DMV records; procedures to protect confidentiality; disclosure
VC 1808.5 – *(Information Release)* DMV records; confidentiality
VC 2431 – *(CORI)* Access to CLETS by CHP for tow truck driver applicants
VC 10500 – *(Vehicles)* Requirement to report stolen vehicles or plates
VC 10551 – *(Reports)* Requirement to report stolen boat to DOJ
VC 10851 – *(Vehicles)* Vehicle theft
VC 20002 – *(Collision Reports)* Accident reporting requirement
VC 20008 – *(Reports)* Traffic accident report required to be submitted to CHP
VC 20012-15 – *(Collision Reports)* Traffic accident reports; disclosure
VC 22650 – *(Vehicles)* Vehicle removal requirement
VC 22651 – *(Vehicles)* Vehicle removal; circumstances allowing
VC 22852 – *(Vehicles)* Notice to owner of towed vehicle
VC 22853 – *(Reports)* Requirement to report stored vehicle to DOJ when unable to establish owner

WELFARE AND INSTITUTIONS CODE
WI 204 – *(CORI)* Transmittal of information relating to arrest of minor; disposition
WI 209-210 – *(Reports)* Detention of minors reporting
WI 361.4 – *(CORI)* Providing CORI obtained by CLETS to a county child welfare agency
WI 601.5 – *(CORI)* Access to CORI at-risk programs for juveniles
WI 781 – *(Juvenile Records, Records Sealing/Destruction)* Authority to require sealing; requirement to seal criminal record
WI 826-826.5 – *(Juvenile Records, Records Sealing/Destruction)* Release, destruction, reproduction of court records
WI 827-828 – *(Juvenile Records)* Court jurisdiction over juvenile records; police authority to release
WI 830 – *(Child Abuse)* Child abuse; disclosure
WI 5328 – *(Information Release)* Mentally ill persons; record confidentiality
WI 8100-8103 – *(Licensing)* Prohibits firearm sales to mentally unfit
WI 15610-32 – *(Elder Abuse)* Definition; reporting and employee requirements
WI 15633 – *(Elder Abuse)* Protects elder abuse and/or dependent adult abuse reports

LEGAL REFERENCE
(By Topic)

AUDITS
28 CFR 20.1 – Justice System Improvement Act; need for CORI audits
California Code of Regulations, Title II, Division 1, Chapter 7, Article 1, subsections 703(d) and 707(b) – *(Audits)* Established requirements for DOJ audit of CORI dissemination

CAMPUS STATISTICS
20 USC 1092(f) – Clery Act

CHILD ABUSE
PC 11166 – Reporting requirements
PC 11167 – Child abuse reports; disclosure
PC 11167.5 – Protects child abuse reports
PC 11169 – Written notifications to suspect of report to child abuse central index
WI 830 – Child abuse; disclosure

CITATIONS
PC 853.6(g) – Citations; booking required on recordable offenses

CLETS
GC 15150-67 – Establishes California Law Enforcement Telecommunications System

CORI
California Code of Regulations, Title II, Division 1, Chapter 7, Article 1, subsections 703(d) and 707(b) – *(Audits)* Established requirement for DOJ audit of CORI dissemination
LC 432.7-432.8 – Regulates disclosure for employment, penalties for violation
LC 432.7(b) – Arrest and detention of peace officer
PC 11075-81 – Definition; dissemination; requirements to regulate dissemination
PC 11078 – Requirement to maintain listing of agencies to which CORI is released
PC 11105 – Requirements/restrictions in furnishing state summary information.
PC 11105.02 – Screening of concessionaires; CORI provided to local government
PC 11105.03 – Public housing authorities; access to information
PC 11105.3 – Youth organizations and human resource agencies access to state CORI for employment/volunteers
PC 11105.4 – Security organizations access to state and local CORI for employment
PC 11105.6 – Bail bond agents access to CORI
PC 11120 – Record defined
PC 11122-23 – Application to obtain copy of own record; submission of application; fee
PC 11124 – Determination of existence of record; copy of record or notice of no record; delivery
PC 11125 – Prohibition from requiring subject to obtain copy of state record

PC 11126 – Procedure for correction/clarification of state record
PC 11127 – Requirement for DOJ to adopt regulations
PC 11140 – Definition of state record
PC 11141-43 – Penalties for unauthorized possession/dissemination of state summary records
PC 11144 – Dissemination for statistical/research purposes; authorized and defined; state
PC 13102 – CORI definitions
PC 13202 – Dissemination for statistical/research purposes; local CORI
PC 13300-01 – Requirements/restrictions in furnishing local summary information
PC 13302-04 – Penalties for unauthorized possession/dissemination of local summary records
PC 13305 – Dissemination for statistical/research purposes; local CORI
PC 13320-23 – Right to examine and challenge state record; fees and procedures
PC 13324 – Procedure for correction/clarification of local record
PC 13325 – Requirement for local record review
PC 13326 – Prohibition from requiring subject to obtain copy of local record
VC 2431 – Access to CLETS by CHP for tow truck driver applicants
WI 204 – Transmittal of information relating to arrest of minor; disposition
WI 361.4 – Providing CORI obtained by CLETS to a county child welfare agency
WI 601.5 – Access to CORI B at-risk programs for juveniles

COLLISION REPORTS
VC 20002 – Accident reporting requirement
VC 20012-15 – Required traffic accident reports, disclosure

COMPLAINTS
PC 832.5 – Citizen's complaints against agency personnel

COMPUTER SYSTEMS
PC 502 – Theft from, malicious access/damage; penalties

CRIMINAL PROCEDURES
PC 691 – Accusatory pleading defined
PC 806 – Examination before magistrate
PC 988 – Arraignment

DETENTION ONLY
PC 849.5 – Arrest deemed detention only, requirements
PC 851.6(a) – Detention certificate requirements

DISPOSITIONS
PC 11115 – Arrest and court action dispositions requirements
PC 13151 – Arrest and court action disposition requirements

DOMESTIC VIOLENCE
PC 13700-02 – Domestic Violence Act

ELDER ABUSE
WI 15610-32 – Definition; reporting and employee requirements
WI 15633 – Protects elder abuse and/or dependent adult abuse reports

FINGERPRINT CARDS
PC 11109 – Coroner's records; decedent fingerprint cards required

FIREARMS
PC 18250 – Notification of retention or destruction of firearms
PC 26180(a) – CCW license application, fingerprints, fees

INFORMATION RELEASE
BP 6054 – Cooperation; assistance with State Bar
California Constitution, Article I, Section 28(b) (Marcy's Law) – Copies of protected documents to Board of Control
CC 1798.32-.44 – Right of inquiry inspection of personal information
CC 1798.53 – Intentional disclosure; Civil action
EVC 250-260 – Definitions; writings; original; duplicate
EVC 1040 – Privilege/conditions for refusal to disclose information
EVC 1270 – Defines government as business
EVC 1271 – Admissible writings and exceptions to hearsay rule
EVC 1506 – Copy of public writing
EVC 1507 – Copy of recorded writing
EVC 1508 – Other secondary evidence of writings
EVC 1509 – Voluminous writings
EVC 1530-32 – Official writings
FC 777.5 – Release of information to banks for employment
FC 6525 – Release of information to financial assistants for employment
FC 14409.2 – Release of information to credit unions for employment
GC 6200-01 – Penalty for theft, destruction, etc., of public records
GC 6250-6276.50 –CPRA
GC 7920.200 – Effect of prior rights and proceedings
GC 7922.530 – Copies of records/time requirements and extensions
GC 7923.000 – Public recourse for failure to provide information requested
GC 7923.650 – Disclosure to prosecuting attorney
GC 13951 – Definitions (victim, injury, crime)
GC 27491.8 – Coroner's records
GC 54985-87 – Fees
HS 1522(a) – Access to CORI by Department of Social Services
HS 1522.06 – Providing CORI obtained by CLETS to a county child welfare agency
PC 146(b) – Simulating official inquiries
PC 168 – Release of felony warrants
PC 293 – Victims of sex offenses may request that names not be disclosed

PC 530.5 – Willful use of personal identifying information; records to reflect innocence of person whose identity was falsely used
PC 841.5 – Confidentiality of victim and witness information
PC 13101 – Criminal justice agencies defined
PC 13104 – Certified reproduction of any record
VC 1808.45-1808.47 – DMV records; procedures to protect confidentiality; disclosure
1VC 1808.5 – DMV records; confidentiality
WI 5328 – Mentally ill persons; record confidentiality

JUVENILE RECORDS
WI 781 – Authority to require sealing; requirement to seal; criminal
WI 826-826.5 – Release, destruction, reproduction of court records
WI 827-828 – Court jurisdiction over juvenile records; police authority to release

LICENSING
BP 21625-28 – Secondhand dealer licensing requirements/reporting
PC 12070-77 – Firearms dealers; dealer record of sales
WI 8100-8103 – Prohibits firearm sales to mentally unfit

MARIJUANA
HS 11356(e) – Juvenile possession on school grounds
HS 11361-61.5 – Purge requirements
HS 11361.7 – Accuracy, timeliness and completeness of destruction; application

MISSING PERSONS
PC 14200-13 – Reporting requirements

PEACE OFFICERS
PC 832.7-832.8 – Peace officer records; confidentiality

PHOTOGRPAHS
CP 129 – Restricts release of photographs of deceased persons

PITCHESS MOTIONS
EVC 1043 – Establishes guidelines for discovery/disclosure of peace officer records

PREMISE VIOLATIONS
BP 24202 – Requirement to report arrest to ABC

PROBATION
PC 1203 – Authority to grant; conditions of probation
PC 1203.4 – Discharged probationer; conviction set aside; reimbursement of county costs

PROPERTY
PC 11108 – Requirement to submit reports of lost, found, or stolen property that is serialized

RECORDS CHECK
EDC 10911.5 – Public recreation employees; fingerprinting
EDC 35021.1 – Automated records check volunteer aids/sex offenses; conviction
EDC 45125 – Requirement for fingerprints/state criminal history check
EDC 88024 – Requirements for fingerprints/state criminal history check; community colleges

RECORDS SEALING/DESTRUCTION
EDC 35254 – Destruction of school district records; microfilming
GC 14745-46 – Destruction of state records; authority
GC 26201-02 – Destruction of county records; authority
GC 26205 – Destruction of certain records; conditions
GC 34090-90.5 – Destruction of city records; authority
GC 34090.6 – Destruction of communication tapes; authority
GC 34090.7 – Destruction of duplicate records less than two years old
PC 851.7 – Petition to seal a record; minor
PC 851.8-851.85 – Factual innocence; sealing/destruction requirements
PC 13103 – Destruction of original records; conditions
WI 781 – Authority to require sealing; requirement to seal; criminal
WI 826-826.5 – Release, destruction, reproduction of court records

REGISTRANTS
PC 186.30 – Gang registrants
PC 290 – Sex offender registration requirements
PC 457.1 – Arson offender registration requirements

REPORTS
BP 21634 – Stolen non-serialized property report to DOJ
FC 21208 – Pawn/buy reports to DOJ
GC 12525 – Death-in-custody reporting
PC 851.6(a) – Detention reports to DOJ
PC 11107 – Local reports to be furnished to DOJ
PC 13020 – Statistical reporting to Attorney General
PC 13022 – Annual justifiable homicide reporting to DOJ
PC 13023 – Hate crimes reporting to Attorney General
PC 13150 – Reporting requirements to DOJ
VC 10551 – Requirement to report stolen boat to DOJ
VC 20008 – Traffic accident report required to be submitted to CHP
VC 22853 – Requirement to report stored vehicle to DOJ when unable to establish owner
WI 209-210 – Detention of minors reporting

RESTRAINING ORDERS
FAC 6345 – Restraining order expiration dates
PC 166.4 – Violation of a court order, restraining order
PC 273.6 – Violation of domestic violence restraining order

SCHOOL EMPLOYEES
EDC 44237 – Bar from employment for sex/narcotics offenses
EDC 45123 – Bar from employment for sex/narcotics offenses
EDC 45124 – Bar from employment; sexual psychopath
EDC 45125 – Requirement for fingerprints/state criminal history check
EDC 45126 – Duty of DOJ to furnish information
EDC 88022 – Bar from employment for sex/narcotics offenses; community colleges
EDC 88023 – Bar from employment; sexual psychopath; community colleges
EDC 88024 – Requirements for fingerprints/state criminal history check; community colleges
EDC 88025 – Duty of DOJ to furnish information, community colleges
HS 11591-91.5 – Notice to school authorities, controlled substance offenses
PC 291-291.5 – Notice to school authorities of arrest for sex crime

STATUTE OF LIMITATIONS
PC 799-805 – Statute of limitations, criminal

SUBPOENAS
CP 128 – Powers of court; compliance with subpoena
CP 1985-1987 – Defines subpoena and affidavit requirements
CP 2002-2015 – Defines manner of production, mode of testimony, and affidavits offered as testimony
CP 2016-2036 – Discovery
CP 2020.10-2020.510 – Nonparty discovery
CP 2023 – Procedure for a subpoena regarding deposition of witness within this state in foreign actions
CP 2024 – Deposition of witness for an out-of-state witness in actions within this state
EVC 1560 – Compliance with subpoena duces tecum for business records
EVC 1561 – Affidavit accompanying records
EVC 1562 – Admissibility of affidavit and copy of records
EVC 1563 – Witness fees and mileage
EVC 1564 – Personal attendance of custodian and production of original records
EVC 1565 – Service of more than one subpoena duces tecum
GC 68093-97 – Witness fees
PC 1054.5 – Criminal discovery

VEHICLES
VC 28 – Vehicle repossession notification
VC 10500 – Requirement to report stolen vehicles or plates
VC 10851 – Vehicle theft
VC 22650 – Vehicle removal requirement

VC 22651 – Vehicle removal; circumstances allowing
VC 22852 – Notice to owner of towed vehicle