Basic Course Workbook Series

Learning Domain 36

Information Systems

Version 5.0

COMMISSION ON PEACE OFFICER STANDARDS AND TRAINING

Basic Course Workbook Series
Student Materials
Learning Domain 36
Information Systems
Version 5.0

© Copyright 2006
California Commission on Peace Officer Standards and Training (POST)
All rights reserved.

Published 1999
Revised July 2002
Revised January 2006
Correction July 2016
Correction March 2018
Revised July 2025
Revised January 2026

This publication may not be reproduced, in whole or in part, in any form or by any means electronic or mechanical or by any information storage and retrieval system now known or hereafter invented, without prior written permission of the California Commission on Peace Officer Standards and Training, with the following exception:

California law enforcement or dispatch agencies in the POST program, POST-certified training presenters, and presenters and students of the California basic course instructional system are allowed to copy this publication for non-commercial use.

All other individuals, private businesses and corporations, public and private agencies and colleges, professional associations, and non-POST law enforcement agencies in-state or out-of-state may purchase copies of this publication, at cost, from POST as listed below:

From POST's Website:

https://post.ca.gov

Go to *https://post.ca.gov/Download-Student-Workbooks*

POST COMMISSIONERS

The POST Commission forms a balanced group of city and county administrators, law enforcement professionals, educators, and public members. The Governor appoints 15 of the Commissioners, with the advice and consent of the Senate, for three-year overlapping terms. The Speaker of the Assembly and the Senate Pro Tempore also each appoint one Commissioner. The Attorney General is an ex-officio member and serves as the 18th POST Commissioner

Geoff Long- *Chair*
Public Member

Rick Braziel - *Vice Chair*
Educator,
Cal Poly Humboldt

Alan Barcelona
Special Agent,
Department of Justice

Ingrid Braun
Sheriff,
Mono County Sheriff's Office

Jim Cooper
Sheriff,
Sacramento County Sheriff's Office

Justin Doering
Senior Deputy Sheriff,
Ventura County Sheriff's Office

Charles Duggan
City Official

P. Lamont Ewell
Public Member

Kelly Gordon
Chief,
Santa Barbara Police Department

Jacob Johnson
Officer,
California Highway Patrol

Michael Moodian
Public Member

Shannan Moon
Sheriff,
Nevada County Sheriff's Office

Tina Nieto
Sheriff,
Monterey County Sheriff's Office

Freddie Rodriguez
Public Member

Benjamin Therriault
Sergeant,
Richmond Police Department

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

THE MISSION OF POST

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.

THE ACADEMY TRAINING MISSION

The primary mission of basic training is to prepare students mentally, morally, and physically to advance into a field training program, assume the responsibilities, and execute the duties of a peace officer in society.

FOREWORD

The California Commission on Peace Officer Standards and Training sincerely appreciates the efforts of the many curriculum consultants, academy instructors, directors and coordinators who contributed to the development of this workbook. We must also thank the California law enforcement agency executives who allowed their personnel to participate in the development of these training materials.

This student workbook is part of the POST Basic Course Training System. The workbook component of this system provides a self-study document for every learning domain in the Basic Course. Each workbook is intended to be a supplement to, not a substitute for, classroom instruction. The objective of the system is to improve academy student learning and information retention and ultimately contribute to you becoming a peace officer committed to safety, and to the communities you will serve.

The content of each workbook is organized into sequenced learning modules to meet requirements as prescribed both by California law and the POST Training and Testing Specifications for the Basic Course.

It is our hope that the collective wisdom and experience of all who contributed to this workbook will help you, the student, to successfully complete the Basic Course and to enjoy a safe and rewarding career as a peace officer.

MANUEL ALVAREZ, Jr.
Executive Director

TABLE OF CONTENTS

INTRODUCTION I
HOW TO USE THE WORKBOOK II

CHAPTER 1 CALIFORNIA LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEM (CLETS) 1-1

OVERVIEW 1-1
INTRODUCTION TO THE CLETS 1-3
DEPARTMENT OF JUSTICE REQUIREMENTS 1-7
UNAUTHORIZED ACCESS OR USE OF INFORMATION 1-11
CRIMINAL OFFENDER RECORD INFORMATION (CORI) 1-15
CHAPTER SYNOPSIS 1-25
WORKBOOK LEARNING ACTIVITIES 1-26

CHAPTER 2 DEPARTMENT OF JUSTICE INFORMATION AND DATABASES 2-1

OVERVIEW 2-1
THE CRIMINAL JUSTICE INFORMATION SYSTEM (CJIS) 2-3
CRIMINAL HISTORY SYSTEM (CHS) 2-4
WANTED PERSONS SYSTEM (WPS) 2-8
SUPERVISED RELEASE FILE (SRF) 2-11
CALIFORNIA RESTRAINING AND PROTECTIVE ORDER SYSTEM (CARPOS) 2-14
MISSING & UNIDENTIFIED PERSONS SYSTEM (MUPS) 2-17
VIOLENT CRIME INFORMATION NETWORK/SEX AND ARSON REGISTRATION (VCIN/SAR) .. 2-23
STOLEN VEHICLE SYSTEM (SVS) 2-25
AUTOMATED BOAT SYSTEM (ABS) 2-29
AUTOMATED PROPERTY SYSTEM (APS) 2-31
AUTOMATED FIREARMS SYSTEM (AFS) 2-34
MENTAL HEALTH FIREARMS PROHIBITION SYSTEM (MHFPS) 2-37
CHAPTER SYNOPSIS 2-38
WORKBOOK LEARNING ACTIVITIES 2-39

CHAPTER 3 DEPARTMENT OF MOTOR VEHICLES INFORMATION SYSTEM 3-1

OVERVIEW 3-1
DEPARTMENT OF MOTOR VEHICLES SYSTEMS/DATABASES 3-3
VEHICLE/VESSEL REGISTRATION DATABASE (VVRD) 3-7
CHAPTER SYNOPSIS 3-12
WORKBOOK LEARNING ACTIVITIES 3-13

SUPPLEMENTARY MATERIAL S-1

ACRONYMS/ABBREVIATIONS S-2
CLETS NETWORK OVERVIEW TABLE S-7
CLETS NETWORK DIAGRAM S-11

GLOSSARY G-1

Student Workbooks

The student workbooks are part of the POST Basic Course Instructional System. This system is designed to provide students with a self-study document to be used in preparation for classroom training.

Regular Basic Course Training Requirement

Completion of the Regular Basic Course is required, prior to exercising peace officer powers, as recognized in the California Penal Code and where the POST-required standard is the POST Regular Basic Course.

Student Workbook Elements

The following elements are included in each workbook:

- Chapter contents, including a synopsis of key points,
- Supplementary material, and
- A glossary of terms used in this workbook.

Introduction

This workbook provides an introduction to the training requirements for this Learning Domain. It is intended to be used in several ways: for initial learning, for test preparation, and for remedial training.

Workbook Format

To use the workbook most effectively, follow the steps listed below.

Step	Action
1	Begin by reading the: Introduction and How to Use the Workbook, which provides an overview of how the workbook fits into the POST Basic Course Instructional System and how it should be used.
2	Refer to the Chapter Synopsis section at the end of each chapter to review the key points that support the chapter objectives.
3	Read the text.
4	Complete the workbook learning activities at the end of each chapter. These activities reinforce the material taught in the chapter.
5	Refer to the Glossary section for a definition of important terms. When first referenced these terms will be bolded and underlined (e.g., **term**).

Chapter 1
California Law Enforcement Telecommunications System (CLETS)

OVERVIEW

Learning Need

Peace officers must know the laws regulating access and use of law enforcement information systems to ensure privacy of individuals, and the integrity and security of the information.

Learning Objectives

The chart below identifies the student learning objectives for this chapter.

After completing study of this chapter, the student will be able to:	Objective ID
• Recognize the requirements of the Department of Justice regarding the confirmation of information obtained from the CLETS network	36.01.2
• Recognize crimes involving unlawful access or use of a law enforcement computer system	36.01.3
• Recognize requirements for authorized release of Criminal Offender Record Information (CORI) based on right-to-know and need-to-know	36.01.4

Learning Objectives (Continued)

After completing study of this chapter, the student will be able to:	Objective ID
• Recognize crimes related to the unauthorized release, receipt, or use of CORI including: - Furnishing the information to an unauthorized person - Lawfully receiving the information and then furnishing it to an unauthorized person - Purchase, receipt, or possession of the information by an unauthorized person	36.01.5 36.01.6 36.01.7

In This Chapter

This chapter focuses on crimes related to the laws and regulations related to the use of law enforcement information systems. Refer to the chart below for specific topics.

Topic	See Page
Introduction to the CLETS	1-3
Department of Justice Requirements	1-7
Unauthorized Access or Use of Information	1-11
Criminal Offender Record Information (CORI)	1-15
Chapter Synopsis	1-25
Workbook Learning Activities	1-26

Introduction

Access to accurate, timely, and complete information is essential to enhance officer safety and allow peace officers to carry out their day-to-day activities and duties.

Leadership

With so much information available to them, peace officers have an obligation to know the requirements for access to, proper use of, and the laws that regulate the systems. Misuse of information systems is a violation of the law and agency policy. Students must develop a clear understanding of the requirements to protect citizen's information and the penalties for failure to do so.

CLETS

The **California Law Enforcement Telecommunications System (CLETS)** is a high-speed message computer network of local, state, and federal databases and systems. It provides all law enforcement user agencies with the capability of obtaining information directly from state and federal computerized information files and is maintained by the California Department of Justice.

Related Terms

To better understand the laws and regulations regarding access and dissemination of law enforcement information, peace officers need to have a clear and consistent understanding of the legal definitions of the following terms as they pertain to CLETS.

Data means a representation of organized information, knowledge, facts, or concepts collected for a specific purpose. One form of data is the information stored in the memory of a computer or presented on a display device. A collection of like or related data is referred to as a **database**.

Access means to gain entry to, instruct, or communicate with the resources of a computer, a computer system, or a computer network.

Available Systems and Databases

Information systems and databases available to authorized law enforcement agencies through the CLETS network are noted in the following table.

Area	System/Database
State	• Criminal Justice Information System (CJIS) • Department of Motor Vehicles (DMV)
National	• National Crime Information Center (NCIC) • National Law Enforcement Telecommunications System (NLETS)
Other	• Canadian Police Information Center (CPIC)

NOTE: Some local law enforcement agencies may also maintain their own local systems and databases not accessible through CLETS. Local records may contain criminal offender record information and other pertinent information available only within that jurisdiction.

Information Inquiries

Circumstances where an inquiry into the CLETS may be necessary can include, but are not limited to:

- Locating information on lost, stolen, or recovered property including vehicles
- Conducting a preliminary or ongoing criminal investigation
- Identifying prior criminal history records
- Verifying the validity of a restraining order
- Verifying the validity of a driver license, vehicle registration, vessel registration, or occupational license
- Determining if a person is wanted for outstanding warrants
- Determining the status of a person on parole or probation
- Reporting or locating a missing person

Administrative Messages

CLETS also provides a fast and efficient system for the transmission of "**free text**," or **administrative messages** to other agencies within the state.

All CLETS messages are ***confidential and for official use only***. Messages should be brief and concise. Examples of uses of administrative messages via the CLETS network include:

- Requests for record validation
- Requests for prisoner pickup and transportation
- Notices such as law enforcement related meetings, training, or seminar announcements
- Requests for mail-back information from databases
- Information regarding the circumstances surrounding the death of an officer killed in the line of duty

NOTE: Personal messages, profane or obscene language, or excessive or detailed descriptions are *not* appropriate for the CLETS message system.

NOTE: **Terminal Mnemonic (MNE)** is the four-character address (terminal name) assigned by the DOJ/CLETS.

All-Points Bulletin Messages

An **All-Points Bulletin (APB)** is an administrative message that is distributed or received via CLETS to law enforcement agencies in the state.

APBs may include, but are not limited to:

- Major identifiable property items
- Crimes against persons (e.g., murder, rape, etc.) when the suspect's mode of operation or vehicle can be described sufficiently
- Missing persons or "be on the lookout" warnings involving life or death situations, emergencies, or suspected foul play
- Acts of nature affecting public safety or law enforcement capabilities
- Death or funeral notices of personnel on active status killed in the line of duty
- Alerts (e.g. Amber, Silver, Feather, Ebony, Yellow, Blue, etc.)

NOTE: Notifications of traffic warrants, recruitment information or similar non-critical information are not appropriate for APBs.

Agency Policies and Procedures

All users of the databases accessed through the CLETS network must abide by their own agency policies and procedures pertaining to use of the system, how the system is used, and how the confidentiality of the information is protected.

Introduction

Compliance with the privacy and security provisions of state law and the Department of Justice regulations based on state law are essential to maintaining the integrity and security of the information available to peace officers.

Authorized Access

Individuals authorized physical access to CLETS terminal may be:

- Sworn law enforcement personnel
- Nonsworn law enforcement personnel
- Technical or maintenance personnel (noncriminal justice personnel and private vendors)

Authorized users are subject to a background investigation.

Background investigations include at minimum:

- Local records check
- California Department of Justice fingerprint checks
- Federal Bureau of Investigation fingerprint checks (if applicable)

Mobile Access

Electronic devices, mobile applications, and radio transmissions must meet DOJ/FBI minimum security specifications. They should not be used routinely for the transmission of criminal history information. These transmissions by unsecured electronic devices can be intercepted by unauthorized people. However, details of criminal history information may be transmitted in such a manner if an officer determines:

- There is *reasonable cause* to believe the safety of the officer and/or the public is at *significant risk*, ***and***
- There is an *immediate need* for summary criminal history information, ***and***
- Information from other databases (e.g., Wanted Persons, Stolen Vehicles) would *not be adequate*.

Examples of justifiable circumstances:
- A hostage situation
- An armed suspect

Examples of unjustified circumstances:
- Routine traffic enforcement
- Routine investigation

Confidentiality

All members of the criminal justice system have a responsibility to the public of California, the law enforcement community, and each individual's own agency to protect the confidentiality of the information accessible through the CLETS network.

Unauthorized access or misuse of CLETS information can lead to:

- CLETS decertification of officer and/or agency
- Disciplinary action
- Termination
- Criminal action (fine and/or imprisonment)
- Civil action

CLETS Information

When obtaining information, peace officers should recognize that CLETS is a "**pointer system**"; that is, the system provides information but does not guarantee that the information is current or absolutely correct.

Information obtained from CLETS can be used by peace officers to establish or reinforce the *reasonable suspicion* necessary to *lawfully detain a suspect*.

Because the information may be unreliable or unsubstantiated, it is *not sufficient* ***alone*** for establishing the probable cause necessary for law enforcement actions such as conducting a search, seizing property, or placing an individual under arrest.

NOTE: For additional information regarding reasonable suspicion and probable cause, refer to LD 15: Laws of Arrest and LD 16: Search and Seizure.

Confirmation of CLETS Information

Information obtained from CLETS is sufficient for establishing probable cause once its validity and reliability have been confirmed.

Confirmation means checking with the originating agency to determine if the person or the property in question is the same as the person or property originally posted by that agency. Confirmation also establishes if the person or property is still wanted and is probably the same as the person or property being inquired about.

Department of Justice regulations require that officers:

- Make an effort to verify the information and match (e.g., details such as accuracy of a license plate run, date of birth, consistency of the physical description, etc.)
- Ensure that confirmation occurred with the originating agency to verify that the person or property is still wanted
- Obtain confirmation before an arrest or the confiscation of the property in response to the computer match

Failure to Confirm Information

The use of unreliable or unsubstantiated information by an officer when establishing probable cause could lead to unlawful searches or seizures as well as incidents of false arrest.

An officer may be held negligent for not accurately confirming information obtained from CLETS before taking such law enforcement actions.

Examples

During a traffic stop, an officer determined that the vehicle and license plate matched a Stolen Vehicle System (SVS) record as a reported stolen vehicle. After detaining the driver, the officer confirmed the information and found that the vehicle had been recovered but the want had not been cleared from the SVS. The officer released the driver and the vehicle and made sure the vehicle was removed from SVS.

Two officers detained a man who was in a specific area and wearing a jacket similar to the one reported earlier worn by a burglary suspect. The man was not carrying identification but gave the officers his name. By accessing CLETS, the dispatcher informed one of the officers that a man with the same name was wanted for an outstanding burglary warrant from another county. The officers continued to detain the man until the information could be confirmed by the originating agency. By waiting before taking further action, they found out that the man did not match the description or date of birth of the person in the original warrant. When the man was able to account for his whereabouts during the time of the recent burglary as well, the officers allowed him to leave.

Non-example: After making contact with a man in a park after hours, the officer used the man's name and date of birth to try to determine if the man had any outstanding warrants. The officer determined that a man with the same name and from the same town was wanted for a number of outstanding traffic warrants. The officer arrested the man. During processing, it was determined that the physical description of the man arrested and the man referred to in the warrant did not match. The officer was negligent for taking action without establishing sufficient probable cause by first confirming the information.

UNAUTHORIZED ACCESS OR USE OF INFORMATION

Introduction

The security of all computer systems must be safeguarded to protect the privacy of individuals, financial institutions, business concerns, governmental agencies, and other entities who lawfully utilize the information provided.

Ethics

Along with the rapid expansion of information systems and their easy access, comes an expanded ethical responsibility. The use of information systems for personal benefit or interest can be a temptation. It is important to talk about the proper use of the systems and strategies to avoid improprieties and indiscretions.

Unlawful Access or Use

If law enforcement personnel access or use information obtained through a computer information system outside that person's normal scope of duties, that person is in violation of *Penal Code Section 502*.

Unlawful actions under *Penal Code Section 502* include, but are not limited to, the actions noted in the table starting on page 1-12.

Unlawful Access or Use (Continued)

Any person who knowingly accesses and without permission...	Penal Code Section
• Alters • Damages • Deletes • Destroys • Otherwise uses any: - Data - Computer - Computer system - Computer network • For personal gain in order to: defraud, deceive, extort, etc. • Or wrongfully control or obtain money, property, or data.	*502(c)(1)*
• Takes • Copies • Or makes use of any data from a: - Computer - Computer system - Computer network; • Or takes or copies any supporting documentation	*502(c)(2)*
• Uses or causes to be used any computer services	*502(c)(3)*
• Adds • Alters • Damages • Deletes • Destroys • Any: - Data - Computer software - Computer programs	*502(c)(4)*

Unlawful Access or Use (Continued)

Any person who knowingly accesses and without permission...	Penal Code Section
• Disrupts or causes the disruption of computer services, or • Denies or causes the denial of computer services to an authorized user	*502(c)(5)*
• Provides or assists in providing a means of accessing a: - Computer - Computer system, or - Computer network	*502(c)(6)*
• Accesses or causes to be accessed any: - Computer - Computer system, or - Computer network	*502(c)(7)*
• Introduces any computer contaminant into any: - Computer - Computer system, or - Computer network	*502(c)(8)*

Consequences

Any person who violates *Penal Code Section 502* can be subject to:

- Criminal prosecution
- Civil liability
- Agency disciplinary action

Examples

A peace officer who was interested in a particular young woman accessed the DMV information system through CLETS to obtain the woman's address. The peace officer then contacted the woman and invited her to dinner. When the woman found out how the peace officer had obtained her address, she filed a complaint with the agency. The peace officer was placed on administrative leave while the agency investigated a violation of *Penal Code Section 502*.

A dispatcher accessed her agency's computer information system and modified the system to indicate an inactive warrant rather than an active warrant for her son. The woman's actions were in violation of *Penal Code Section 502(c)(4)*. She was fired from her job when the offense was discovered. The agency filed charges and referred the case to the district attorney for prosecution.

Non-example: A peace officer on patrol came upon a minor traffic accident scene where both drivers were arguing about who was at fault. The peace officer was able to intercede and convinced the men to exchange information and let their respective insurance companies handle the problem. Even though the accident was below the minimum reporting level, the peace officer decided to check each person's driver license and vehicle registrations to assure that each driver was providing the other with valid information. The peace officer's use of the law enforcement information system was not in violation of the law.

CRIMINAL OFFENDER RECORD INFORMATION (CORI)

Introduction

The California Department of Justice and local law enforcement agencies maintain summaries of criminal histories. These summaries of criminal history records are commonly referred to as "**rap sheets**."

CORI

Criminal Offender Record Information (CORI) refers to the records and data compiled by criminal justice agencies for the purpose of identifying criminal offenders. *(Penal Code Section 11075)*

The information summarized under CORI may include the offender's:

- Name
- Date of birth
- Physical description
- Fingerprints
- Photographs
- Summary of arrests
- Pretrial proceedings
- The nature and disposition of criminal charges
- Sentencing
- Incarceration
- Rehabilitation (parole/probation)
- Release

Access to CORI

CORI can be accessed from a number of different computer systems: local, state, or national. Information can also be stored and retrieved as hard copy (paper) files as well.

NOTE: Electronic devices, mobile applications and radio transmissions should not be used for the transmission of Criminal Offender Record Information except under certain specified conditions. For additional information, refer to the lesson *Access to Information* in this chapter.

State CORI

Master records of identification and CORI are compiled by the Attorney General and maintained by the Department of Justice. *(Penal Code Section 11105(a))*

CORI does not refer to records and data compiled by criminal justice agencies other than the local agency or the Attorney General. Nor does it refer to records of complaints to, or investigations by, the local agency or the Attorney General, or to records of intelligence information or security procedures.

NOTE: Collection and release of information from the Federal Bureau of Investigation (FBI) is governed by the FBI.

Local CORI

Local agencies may also maintain their own master records of CORI. Local criminal history information may be in a hard copy (paper) manual and/or automated formats for use within that specific jurisdiction. *(Penal Code Section 13300(a))*

Release of CORI

Both state and local CORI should be considered private information. Individuals have the expectation that such information about themselves will not be given unless there is an authorized reason to do so.

Before releasing state or local CORI, an agency must first determine if the person or agency requesting the information is authorized to receive the information. *(Penal Code Section 11105(b), and 13300(b))*

Right-to-Know, Need-to-Know

State or local CORI can be released only if the requesting person or agency:

- Is *authorized by law* to receive the information (**right-to-know**), and
- Has a *compelling reason* to request the information (**need-to-know**.)

In order to gain access to CORI, a requesting individual or agency must have the:

- *Right or authority* to obtain CORI pursuant to:
  - A court order
  - Statutory law
  - Case law, **and**
- A compelling *need* to obtain CORI in order to execute official responsibilities

Examples:
- Probation or parole officers in the course of their responsibilities to supervise specific individuals
- Public defenders or attorneys of record preparing to defend an individual
- Peace officers who are conducting a specific investigation

NOTE: Users are not authorized to access CORI for licensing, employment, or certification purposes.

Community Policing

All peace officers must keep in mind that a public office is a public trust. Accordingly, agency time and resources must never be used to further personal gain. The misuse of computer equipment and access to confidential information is one of the most common ways that officers have found to violate public trust and thereby ruin their careers and bring shame to the agency.

State "Authorized Agency" List

The Attorney General provides a list of agencies or individuals who shall or may have access to state CORI for employment, licensing, certification, or criminal investigation purposes. This list, based on the right-to-know and need-to-know, is commonly referred to as the "authorized agency" list. *(Penal Code Sections 11105(b)* and *(c))*

This list should not be used to determine if an agency or individual should have access to a specific arrest or crime report.

Examples of authorized agency personnel include but are not limited to:

- Peace officer
- Dispatcher
- Records clerk
- Evidence staff

NOTE: If an agency is not certain it can furnish a copy of an arrest or crime report involving an adult, the agency should contact their legal counsel.

Access to One's Personal CORI

The subject of a state or local CORI is allowed to obtain a copy of that individual's own record in order to ensure the accuracy of the record and to refute any erroneous information contained in the record. *(Penal Code Sections 11120-11127 and 13320-13326)*

To obtain a copy of an individual record, that person must:

- Complete an *application to obtain a copy of the State Summary Criminal History Record*
- Submit applicant fingerprint cards
- Pay a fee to the Department of Justice

Juvenile Information

The presiding judge of the Juvenile Court in each county dictates who can receive the names and addresses of juveniles named in reports. This action is commonly referred to as a TNG Order and can vary from county to county.

NOTE: "TNG" refers to the initials of the juvenile in the case that established precedent pertaining to such orders.

Unauthorized Release or Use of CORI

Release or receipt of local or state CORI without legal authority is a crime. The following table identifies such actions.

Crime	Crime Elements	*Penal Code Section*
Furnishing CORI to an unauthorized person	• Any employee - Of a criminal justice agency, or - The Department of Justice • Who knowingly • Furnishes a record or information obtained from a record • To a person who is *not authorized by law to receive* the record or information • Is guilty of a misdemeanor	*11141* (state CORI)
		13302 (local CORI)
Lawfully receiving CORI and then furnishing the information to an unauthorized person	• Any person • *Authorized by law to receive* a record or information obtained from a record • Who knowingly • Furnishes the record or information obtained from a record • To a person who is *not authorized by law to receive* the record or information • Is guilty of a misdemeanor	*11142* (state CORI)
		13303 (local CORI)

Unauthorized Release or Use of CORI (Continued)

Crime	Crime Elements	*Penal Code Section*
Unauthorized purchase, receipt, or possession of CORI	• Any person who • Knowing he is not authorized by law to receive a record or information obtained from a record • Knowingly: - Buys - Receives - Possesses • The record or information • Is guilty of a misdemeanor NOTE: Publishers, editors, reporters, or other people employed by print, radio, or television news media may be exempt from this section. *(Evidence Code Section 1070)*	*11143* (state CORI) *13304* (local CORI)

Misuse of CORI

The Criminal Records Security Unit of the Department of Justice conducts routine audits to ensure that CORI is accessed and used appropriately. This unit also handles complaints from private citizens regarding the misuse of a subject's record.

If misuse of the CORI is discovered, the Department of Justice requests that disciplinary action be taken. If the misuse is severe, authorized individuals or agencies may lose direct access to the CORI maintained by the Department of Justice.

Individuals who misuse the system or the information may be subject to discipline based on:

- Local agency policies and procedures
- Personal punitive damages paid by the employee or the employee's agency
- Criminal prosecution

Examples

In the course of a burglary investigation, the investigating officer requested access to two suspects' local CORI. The investigating officer was attempting to find out if either suspect had a record of arrests for similar crimes in the past. The investigating officer had both the "right-to-know" and "need-to-know" the information and therefore was allowed access to both suspects' records.

Non-example: A private investigator made arrangements with a peace officer to have the peace officer access law enforcement records whenever the investigator needed information. The investigator agreed to pay the peace officer for the information and promised that the peace officer could join his firm once the peace officer retired. Both men committed criminal acts: the peace officer for furnishing the information and the investigator for unauthorized receipt of the information.

Additional Statutes

The following table identifies additional statutes related to access and dissemination of CORI:

Description	Penal Code Section
Dissemination to authorized agencies	*11076*
Attorney General duties	*11077*
Listing of agencies to whom information is released or communicated	*11078*
Investigations, cooperation by agencies	*11079*
Right of access of information authorized by other provisions of law	*11080*
Federal parolees residing or domiciled in city or county request for information by chief or police or sheriff	*11080.5*
No access on information unless otherwise authorized by law	*11081*
State summary criminal history information; person entitled to receive a record	*11105.1*
Definition of “record”; person authorized by law to receive a record	*13301*
Request of employee to obtain record or notification of existence of record; prohibition; violations; penalty	*13326*

Additional Statutes (Continued)

Description	Additional Code Section
Unauthorized disclosure of information from any agency record	*Vehicle Code Section 1808.45*
Obtaining information from agency files using false representations	*Vehicle Code Section 1808.46*
Release of information from accident reports	*Vehicle Code Sections 20008-20012*
Theft, destruction, falsification, or removal by officer custodian	*Government Code Section 6200*
Theft, destruction, falsification, or removal by person other than officer custodian	*Government Code Section 6201*
Release of information from an individual's crime or arrest reports	*Government Code Sections 6251-6255*
Limited Criminal History Information	DOJ Information Bulletin A-85-CIIB
Access to Criminal Offender Record Information	DOJ Information Bulletin MC-90-03-BJIS

Learning Need

Peace officers must know the laws regulating access and use of law enforcement information systems to ensure privacy of individuals, and the integrity and security of the information.

DOJ Requirements [36.01.2]

Department of Justice regulations establish requirements to be followed by officers to ensure accuracy of their data.

An officer may be held negligent for not accurately confirming information obtained from CLETS before taking such law enforcement actions.

Unauthorized Access or Use of Information [36.01.3]

If law enforcement personnel access or use information obtained through a computer information system outside that person's normal scope of duties, that person is in violation of *Penal Code Section 502*.

Right-to-Know, Need-to-Know [36.01.4]

In order to gain access to state or local CORI, the requesting individual or agency must have a right-to-know and a need-to-know.

Unauthorized Release or Use of CORI [36.01.5, 36.01.6, 36.01.7]

The release, receipt, or use of state or local CORI without legal authority is a crime.

Introduction

To help you review and apply the material covered in this chapter, a selection of learning activities has been included. No answers are provided. However, by referring to the appropriate text, you should be able to prepare a response.

Activity Questions

1. When Jones was 20 years old, he was convicted of misdemeanor battery and was arrested once for DUI. He pleaded no contest. Now at 35, Jones has been an exemplary citizen for 10 years. After being turned down for a job, Jones asked his friend, Smith, a probation officer, to find out if his criminal history records have any errors that may have cost him the job. Smith accessed Jones's CORI through CLETS the next day and found out that the date of the battery conviction was listed erroneously as last year. Smith made a copy of the record and gave it to Jones. What, if any, crime(s) have been committed and by whom? Explain.

2. Why does transferring criminal record information over an electronic device or mobile application pose a risk to security and privacy?

Activity Questions (Continued)

3. Officer Sally Jones was assigned to conduct an assault with a deadly weapon (P.C. 245) investigation. She identified the suspect, ran his name through state and local criminal history computer systems, and discovered that he had numerous arrests and convictions for violent assaults. Officer Jones also recognized that the suspect lived in her apartment complex and was dating her next-door neighbor, Mary. When Officer Jones got off duty and arrived home, she met her husband Mark Jones, a Deputy Sheriff. Officer Jones explained the case to her husband and told her husband that she was concerned about the safety of Mary because of the violent tendencies of the suspect. Officer Jones was considering telling Mary about the suspect's arrests and convictions so that she could make a rational decision about dating the suspect.

   A. Was it lawful for Officer Jones to share the CORI information with Deputy Jones? Explain your answer.

   B. Would it be lawful for Officer Jones to share the CORI information about the suspect with Mary in order to protect her safety? Explain your answer.

Activity Questions (Continued)

4. Explain the difference between “right-to-know” and “need-to-know” as the last pertains to CORI. Give an example to illustrate the distinction.

Chapter 2
Department of Justice Information and Databases

OVERVIEW

Learning Need

Peace officers must know the requirements for access and entry into the appropriate Department of Justice information systems and databases available on the CLETS network to perform their duties for their safety and the safety of others.

Learning Objectives

The chart below identifies the student learning objectives for this chapter.

After completing study of this chapter, the student will be able to:	Objective ID
• Identify systems and databases available from the Criminal Justice Information System (CJIS) and the types of information provided	36.02.1
• Recognize the minimum information required for generating an inquiry into each of the CJIS systems and databases	36.02.12

In This Chapter

This chapter focuses on law enforcement information systems available through the CLETS network. Refer to the chart below for specific topics.

Topic	See Page
The Criminal Justice Information System (CJIS)	2-3
Criminal History System (CHS)	2-4
Wanted Persons System (WPS)	2-8
Supervised Release File (SRF)	2-11
California Restraining & Protective Order System (CARPOS)	2-14
Missing & Unidentified Persons System (MUPS)	2-17
Violent Crime Information Network/Sex & Arson Registration (VCIN/SAR)	2-23
Stolen Vehicle System (SVS)	2-25
Automated Boat System (ABS)	2-29
Automated Property System (APS)	2-31
Automated Firearms System (AFS)	2-34
Mental Health Firearms Prohibition System (MHFPS)	2-37
Chapter Synopsis	2-38
Workbook Learning Activities	2-39

THE CRIMINAL JUSTICE INFORMATION SYSTEM (CJIS)

Introduction

The **Criminal Justice Information System (CJIS)** network is a computerized system containing records that are of interest to the criminal justice community. The CJIS is maintained by the California Department of Justice in Sacramento. It is available to local, state, and federal criminal justice agencies through the CLETS network.

Available Databases

There are a number of databases available within CJIS.

	System Name	Acronym/ Abbreviation
Persons	Wanted Persons System	WPS
	Criminal History System	CHS
	California Restraining and Protective Order System	CARPOS
	Missing and Unidentified Persons System	MUPS
	Supervised Release File	SRF
	Violent Crime Information Network/Sex and Arson Registration	VCIN/SAR
	Mental Health Firearm Prohibition System	MHFPS
Property	Stolen Vehicle System	SVS
	Automated Boat System	ABS
	Automated Property System	APS
	Automated Firearms System	AFS

Introduction

The Criminal History System (CHS) contains criminal history information that is available to criminal justice agencies on a "*right-to-know*" and a "*need-to-know*" basis for the performance of their official duties.

CHS Organization

The CHS is organized into the following three portions.

	Description
Master Name Index (MNI)	• Automated online file containing personal descriptor records of all subjects with criminal and/or applicant records on file with the Department of Justice
Automated Criminal History System (ACHS)	• Centralized automated system designed to provide authorized Criminal Offender Record Information (CORI)
Manual Criminal History System (MCHS)	• Criminal and applicant files that have not been automated • Files can be requested through the Department of Justice Center by telephone, teletype, or mail

Routing Information

When making an inquiry into the CHS, per DOJ mandates, the requesting party must provide the following information before access to the system will be allowed:

- Requesting person's name
- Requesting person's unit or division, and
- Official purpose for the information requested

Inquiries into the CHS to Obtain the CORI

In order to access specific CORI records from the Automated or Manual Criminal History System of the CHS, the requesting person must first have the subject's:

- Criminal Identification and Information Number (**CII**), or
- A disposition number

In order to obtain these numbers, if not already known, the requesting person may have to first access the MNI of the CHS.

Inquiries into the MNI

The following table identifies the information needed to make an inquiry into the MNI.

Inquires based on...	*Minimum* information required	Optional information to narrow search results
Master Name Index (**MNI**)	• Name (**NAM**) • Sex (**SEX**) • Date of Birth (**DOB**) or Age (**AGE**)	• Social Security Number (**SOC**) • FBI Number (**FBI**) • Driver License Number (**DLN**) or Operator's License Number (**OLN**) • California Department of Corrections Number (**DOC**) or California Youth Authority Number (**CYA**)

Identification Numbers

A match from the Master Name Index will include the subject's identification numbers necessary to access other portions of the CHS. The following table further identifies the information provided regarding a subject's identification numbers.

ID Type	Identification Code	Record Type	Description
CII number	CII number preceded by an "A"	Automated	• A record that has been completely automated and is currently maintained in ACHS
	CII number preceded by an "M"	Manual	• A record that is maintained manually only • Must be obtained directly from the Department of Justice
	CII number preceded by an "H"	Hybrid	• A record that is only partially automated • Part of the record is in a manual format
Disposition number	All numeric	DSP	• A record that is based solely on information obtained from disposition records • Not verified by fingerprint comparison

Classifications

The following table identifies the crime classifications that are generally recorded in the ACHS.

Classification	Retention period
Misdemeanor arrests (with or without conviction)	10 years from date of arrest
Felony arrests (without conviction)	
Misdemeanor priors (misdemeanor conviction where a prior conviction constitutes a felony)	Until the subject is 70 years old
Felony convictions	
Subjects convicted of registerable sex offenses *(Penal Code Section 290)*	Until the subject is 100 years old

Introduction

The **Wanted Persons System (WPS)** is a file of records pertaining to wanted fugitives and arrest warrants. WPS records retained in the system longer than 72 hours must be based on an arrest warrant. These warrants are maintained by state, local, and federal criminal justice agencies in California.

A match made on a WPS record *does not, by itself, provide sufficient grounds to arrest a person*. Confirmation of the information is necessary. Agencies must respond to a confirmation request within 10 minutes on a 24-hour basis.

Levels of Warrants in the WPS

The WPS warrant records are categorized as felony or misdemeanor.

Temporary warrants can be placed in WPS prior to actual issuance of the warrant. They are retained for 48-72 hours and purged from the system if not modified to a permanent status.

NOTE: Felony and serious misdemeanor records are also forwarded to the National Criminal Information Center (NCIC).

Inquiries into the WPS

Inquiries into the WPS may be made by using a subject's name and physical descriptors or by using numeric identifiers. More hits (positive responses) may be obtained by a name search than by searches based on numeric identifiers.

The following table identifies the requirements for each type of inquiry into the WPS.

Inquires based on...	*Minimum* information required	Optional information to narrow search results
Name and physical descriptors	• Name (**NAM**) • Sex (**SEX**)	• Age (**AGE**) • Date of Birth (**DOB**) • Race (**RAC**) • Height (**HGT**) • Weight (**WGT**)
Numeric identifiers	One or more of the following may be used. • Criminal Identification and Information Number (**CII**) • FBI Number (**FBI**) • Driver License Number (**DLN**) • Social Security Number (**SOC**) • Miscellaneous Identification Number (**MNU**)	• Name (**NAM**) • Sex (**SEX**) • Date of Birth (**DOB**)

Caution Codes

Positive matches may include caution codes which have been entered to indicate special handling of the subject.

Caution codes may include, but are not limited to:

- Armed and dangerous
- Mentally disturbed
- Suicidal tendencies
- Escape risk

Introduction

The **Supervised Release File (SRF)** was developed by the Department of Justice to improve the supervision of convicted persons, enhance officer safety, and assist in investigations.

The SRF contains brief but informative indexes to the supervising agency's more complete records. Responses from the SRF may disclose vital information regarding individuals that have a history of involvement with the criminal justice system.

Types of Records in the SRF

The following table identifies the types of records included in the Supervised Release File.

Records pertaining to...	Entered by...
• California Department of Corrections and Rehabilitation (CDCR) parolees	• California Department of Corrections and Rehabilitation
• California Division of Juvenile Justice (DJJ) parolees	• California Division of Juvenile Justice
• Probationers/Post Release Community Supervision (PRCS) Subjects	• County probation agencies
• Federal parole and probation records	• Individual federal agencies

NOTE: Federal probation records can be found in NCIC and SRF.

Contact Messages

The SRF also allows peace officers to send information about an encounter with a subject. These contact messages allow for a means of tracking supervised individuals and also can serve as an investigative tool.

Contact messages are transmitted to the Department of Justice, connected to the appropriate record, and then forwarded to the agency that originally entered the record.

The contact message may contain:

- The date and time of the contact
- The officer and agency who made the contact
- A call back telephone number
- The status of any enforcement action taken
- Vehicle data
- A brief summary of the nature of the contact

Inquiries into the SRF

The following table identifies the information required to make an inquiry into the SRF.

Inquires based on...	*Minimum* information required	Optional information to narrow search results
Name and physical descriptors	• Name (**NAM**) • Physical descriptors such as: - Sex (**SEX**) - Race (**RAC**), etc.	• California Identification and Information Number (**CII**) • Social Security Number (**SOC**) • Driver License Number (**DLN**) or Operator's License Number (**OLN**)

NOTE: Inquiries into SRF are also automatically forwarded to the WPS and the California Restraining and Protective Order System for further searches.

Responses from the SRF

Responses from the SRF can be full or abbreviated. A typical positive response may provide the following information regarding the subject:

- Physical descriptors
- Driver license number
- Social security number
- County and city of residence
- Primary offense
- Sex registration status
- Supervising officer's name, phone number, and unit

Advisory Information

Advisory information (i.e., warnings) is also included in a response when such information is deemed critical and for the immediate knowledge of any law enforcement officer who makes contact with the subject

CALIFORNIA RESTRAINING AND PROTECTIVE ORDER SYSTEM (CARPOS)

Introduction

The **California Restraining and Protective Order System (CARPOS)** is a system that identifies restraining and protective orders entered into CLETS by law enforcement agencies. Law enforcement agencies can access this system for the purpose of obtaining the terms and conditions of a specific restraining order on an individual.

Restraining Orders

The CARPOS maintains information regarding the restraining orders that must be enforced throughout the state. These include:

- Certain family law domestic violence case orders
- Criminal restraining orders
- Civil orders
- Juvenile orders
- Out-of-state domestic violence orders that have been registered with the clerk of the county superior court

NOTE: Out-of-state restraining orders can be located in NCIC.

Firearms Restrictions

The CARPOS contains a listing of restraining orders which prohibit the purchasing or receiving of a firearm. *(Penal Code Section 12021(g))*

This information is also used by the Department of Justice Dealer's Record of Sale Unit for firearm sales purposes.

Mandated Restraining Orders

- Emergency Protective Order (EPO)
- Order to Show Cause and Temporary Restraining Order (TRO)
- Restraining Order After Hearing (OAH)
- Restraining Order-Juvenile
- Temporary Restraining Order (Attachment to Order to Show Cause)
- Order to Show Cause (Harassment of Employee) and Temporary Restraining Order
- Order After Hearing on Petition for Injunction Prohibiting Harassment of Employee
- Protective Order in Criminal Proceeding
- Order to Show Cause (Harassment) and Temporary Restraining Order
- Order After Hearing on Petition for Injunction Prohibiting Harassment
- Out-of-State Domestic Violence Protective Order
- Gun Violence Restraining Order (GVRO)

NOTE: A restraining or protective order will remain in CARPOS until midnight of the date of expiration or until the entering agency cancels the record, whichever is first.

NOTE: There are other types of restraining orders that are not mandated by law for entry into CARPOS but are also included.

Inquiries into the CARPOS

The following table identifies the information required to make an inquiry into the CARPOS.

Inquires based on...	*Minimum* information required	Optional information to narrow search results
Name and physical descriptors	• Name (**NAM**) • Sex (**SEX**)	• Date of Birth (**DOB**) or Age (**AGE**) • Race (**RAC**) • Height (**HGT**) • County or Region (**CNT**)
Other information	• File Control Number (**FCN**)	

NOTE: Responses from the CARPOS may also be returned when an inquiry is made directly into the WPS or into the SRF.

MISSING & UNIDENTIFIED PERSONS SYSTEM (MUPS)

Introduction

The **Missing & Unidentified Persons System (MUPS)** is a file of records which catalogs reports of missing or unidentified persons according to a variety of physical (e.g., date of birth, height, weight, hair color, eye color, etc.) and dental characteristics. It is continuously available to law enforcement agencies to assist in locating and recovering missing and unidentified persons.

Missing Persons

Penal Code Sections 14205 and 14206 require that local law enforcement agencies accept any report regarding a missing person (including reports that are called into the agency) without delay.

Agencies are required to..	Additional information
• Forward a copy of the missing persons report	Reports must be forwarded to the: • Agency with jurisdiction over the missing person, • Agency with jurisdiction of the place where the person was last seen, and • Department of Justice's MUPS via the CLETS network
• Broadcast a "**Be-On-the-Look-Out" (BOLO)** bulletin	Bulletins must be broadcast within the jurisdiction if: • The missing person is under 21 years old, or • There is evidence the person is at risk

Missing Persons (Continued)

Agencies are required to..	Additional information
• Provide an information release form to the reporting party	The Department of Justice release form authorizes the release of: • Dental x-rays • Skeletal x-rays • And/or photographs of the missing person
• Enter a missing person into CLETS	If missing person is under 21 years of age or at risk the agency must enter them into CLETS within 2 hours pursuant to *Penal Code Section 14211(e).*

NOTE: Officers must be familiar with and comply with their own agency policies and guidelines regarding reporting missing persons.

NOTE: For more information regarding the MUPS refer to LD 27: Missing Persons

Categories of Missing Persons

The following table identifies categories used for organizing missing persons information within the MUPS.

Category	Description
Runaway	• Children who have left home without permission of a parent or guardian
Lost	• Persons who are lost or have wandered away
Catastrophe	• Persons missing after a catastrophe (e.g., flood, earthquake, etc.)

Categories of Missing Persons (Continued)

Category	Description
Stranger Abduction	• Persons taken by a stranger or nonfamily member
Parental/Family Abduction	• Children taken by a parent or family member
Suspicious Circumstances	• Persons missing under circumstances indicating possible foul play
Unknown Circumstances	• Circumstances surrounding the disappearance are unknown
Missing Adult	• Adults who have left of their own free will
Dependent Adult	• Adults with physical or mental limitations who are missing

Inquiries Regarding Missing Persons

The following table identifies a number of ways an inquiry can be made regarding a missing person.

Inquires based on...	*Minimum* information required	Optional information to narrow search results
Name	• Name (**NAM**) • Sex (**SEX**)	• Date of Birth (**DOB**) or Age (**AGE**) • Race (**RAC**) • Height (**HGT**) • Weight (**WGT**) • Eye Color (**EYE**) • Hair Color (**HAI**) • Last Day of Contact (**DLC**)
Physical descriptors	• Sex (**SEX**) • Date of Birth (**DOB**) or Age (**AGE**) • Race (**RAC**) • Height (**HGT**)	• Weight (**WGT**) • Eye Color (**EYE**) • Hair Color (**HAI**) • Last Day of Contact (**DLC**) • Scars/Marks/Tattoos (**SMT**) • Area (**ARE**)
Other information	• Dental Characteristics (**DCH**)	
	• File Control Number (**FCN**)	
	• Originating Agency Case Number (**OCA**)	
	• Operator's License Number (**OLN**)	
	• Vehicle description information such as: - Vehicle License Number (**VLN**) - Vehicle Color (**VCO**) - Vehicle Make (**VMA**)	

Unidentified Persons

The unidentified persons portion of Missing & Unidentified Persons System contains reports from California and surrounding states about unidentified persons (living or deceased) and body parts. Along with physical descriptions, reports may also include fingerprints and dental charts, if available.

All missing and unidentified persons reports are cross-checked daily and agencies are notified of possible matches.

Categories of Unidentified Persons

The following table identifies categories used for organizing unidentified persons information within the Missing & Unidentified Persons System.

Category	Description
Deceased	• Any unidentified deceased persons
Living Person	• Persons living and unable to ascertain their identities
Catastrophe Victim	• Unidentified catastrophe victims

Inquiries Regarding Unidentified Persons

The following table identifies a number of ways an inquiry can be made regarding an unidentified person.

Inquires based on...	*Minimum* information required	Optional information to narrow search results
Physical descriptors	• Sex (**SEX**) • Race (**RAC**) • Age (**AGE**) • Height (**HGT**)	• Weight (**WGT**) • Eye Color (**EYE**) • Hair Color (**HAI**) • Estimated Date of Death (**EDD**) • Scars/Marks/Tattoos (**SMT**) • Area (**ARE**)
Body parts	• Body Part Status **(BPS)**	• Sex (**SEX**) • Area (**ARE**)
Other information	• Dental Characteristics (**DCH**)	
	• File Control Number (**FCN**)	
	• Originating Agency Case Number (**OCA**)	

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

Introduction

The **Violent Crime Information Network (VCIN)** is a database designed to facilitate the sharing of information related to violent crimes among law enforcement agencies. The network is commonly utilized in criminal justice contexts allowing law enforcement agencies to access and disseminate critical data regarding violent offenses to enhance public safety and investigative efforts.

SAR

The **Sex and Arson Registration (SAR)** is one increment of the VCIN. The SAR maintains a statewide file on convicted persons required to register as sex offenders pursuant to *Penal Code Section 290* or arson offenders pursuant to *Penal Code Section 457.1*.

The SAR provides peace officers with:

- Listings of registrants residing in specific geographic areas
- Assistance in identifying suspects in current sex and arson crimes based on:
  - Physical characteristics
  - Type of offense
  - Geographic location

Information Available From the SAR

The following table provides information regarding the records available on SAR.

Information based on...	Examples
Name and physical characteristics	• Full name • Aliases and monikers • Date of birth • Physical characteristics • Identifying marks (e.g., scars, tattoos, etc.) • Occupation • Operator's license number • Miscellaneous identification numbers • DNA case number
Offenses	• All registration offenses the offender has been convicted of
Registration history	• Current registration date • Address • Other associated addresses (e.g., place of work, etc.) • Vehicle(s) registered to the person

Record Retention

Records of sex offenders convicted of registration offenses *(Penal Code Section 290)* are retained for the offender's lifetime.

Inquiries into the SAR

Inquiries into the VCIN/SAR can be made by using the suspect's:

- Name (**NAM**) and date of birth (**DOB**)
- File Control Number (**FCN**)
- Criminal Identification and Information Number (**CII**)

Introduction

The **Stolen Vehicle System (SVS)** is a database containing records related to vehicles, license plates, and vehicle parts.

Available Information

The following table identifies the type of information that is stored in the SVS.

Information regarding...	That have been...
Vehicles	• Stolen • Lost • Pawned • Repossessed • Impounded (law enforcement hold) • Recovered
License plates	• Stolen • Lost

NOTE: Information regarding vehicles associated with wanted or missing persons is also maintained.

Types of Vehicles Included in the SVS

The information accessible from the SVS pertains to a number of different types of vehicles.

- Automobiles
- Motorcycles
- Motor Scooters
- Mopeds
- Personal trucks
- Farm equipment
- Golf carts
- Commercial Trucks
- Aircraft (except model aircraft)
- E-bikes
- Trailers
- Mobile homes
- Motor homes
- Construction equipment
- Go-carts
- Snowmobiles
- Amphibious vehicles
- All-terrain vehicles
- Motorized wheelchairs

Types of Vehicle Parts in the SVS

Information regarding any serialized component part of a vehicle may also be included in the SVS.

NOTE: Radios and stereo equipment are *not listed as vehicle parts*. Instead, they are listed as property in the Automated Property System of CJIS.

Types of Records in the SVS

There are various types of vehicle records used in the SVS. The following table identifies a number of them along with the record retention period.

Vehicle record	Retention period
• Stolen Vehicle or Part	Balance of year entered plus four years
• Stolen or Lost License Plate(s)	One year past the year of registration
• Found/Evidence Vehicle Part/Plate	Six months
• Pawned Vehicle	Six months
• Felony Vehicle/Plate	90 days
• Missing Person Vehicle	30 days
• Stored Vehicle	30 days
• Impounded Vehicle (stored vehicle with law enforcement hold)	60 days
• Reported Lost Vehicle	30 days
• Repossessed Vehicle	30 days
• Cleared/Recovered Vehicle	30 days
• Located Vehicle	30 days

Inquiries into the SVS

The following table identifies the information required to make an inquiry into the SVS.

Inquiries regarding...	Minimum information required (one or more of the following)
Vehicles/license plates	• License Plate Number (**LIC**) • Vehicle Identification Number (**VIN**) • Engine Number (**ENG**) • **Owner Applied Number** (**OAN**)
Vehicle component parts	• Serial Number (**SER**) • Owner Applied Number (**OAN**)

Introduction

The **Automated Boat System (ABS)** is a database containing records of watercraft that have been reported stolen, lost, repossessed, and stored. It also contains information regarding serialized boat parts that have been stolen.

Types Of Watercrafts Included in the ABS

The information accessible from the ABS pertains to a number of different types of watercrafts.

- Boats
- Ships
- Yachts
- Barges
- Jet Skis
- Wind-powered surfboards
- Motorized surfboards
- Rafts
- Canoes
- Hydrofoils

Types of Vehicle Parts in the ABS

Information regarding any serialized component part of a watercraft may also be included in the ABS.

Types of Records in the ABS

There are various types of boat records used in the ABS. The following table identifies a number of them along with the record retention period.

Boat record	Retention period
• Stolen boat or part	Balance of year entered plus four years
• Stored boat	30 days
• Reported lost boat	30 days
• Repossessed boat	30 days
• Cleared/Recovered boat	30 days
• Located boat	30 days

NOTE: All returns from the database on stored boats will return as impounded boats.

Inquiries into the ABS

The following table identifies the information required to make an inquiry into the ABS.

Inquiries regarding...	Minimum information required (one or more of the following)
Watercraft	• Registration Number/CF Number (**REG**) • Engine Number (**ENG**) • Boat Hull Number (**BHN**) • Owner Applied Number (**OAN**)
Boat parts	• Serial Number **(SER)** • Owner Applied Number (**OAN**)

Introduction

The **Automated Property System (APS)** is a file system containing serialized property records involving property and jewelry.

Available Information

The following table identifies the type of information that is stored in the APS.

Information regarding...	That have been...
Serialized property	• Stolen • Lost • Found • Held for evidence • Under observation • Pawned • Bought
Non-serialized jewelry or property	• Pawned • Bought

Types of Property Included in the APS

The information accessible to law enforcement agencies includes a number of different types of property. The following list identifies these various types of property included in the APS.

- Non-serialized jewelry (pawn/buy)
- Bicycles
- Camera and photography
- Data processing
- Equipment/tools
- Furniture
- Games/gambling apparatus
- Household equipment
- Badges
- Special documents, food stamps/tickets
- Keepsakes/collectibles
- Livestock
- Musical Instruments
- Non-serialized property (pawn/buy)
- Office Equipment
- Personal accessories
- Audio/stereo/television equipment/accessories
- Sports/exercise equipment
- Toxic chemicals
- Viewing equipment
- Well drilling equipment
- Other
- Stolen credit cards/check

Types of Property Records Included in the APS

There are various types of property records used in the APS. The following table identifies a number of them along with the record retention period.

Property record	Retention period
• Stolen credit cards	Six months
• Stolen, lost, evidence, property other than credit cards	Three years
• Under observation and found property other than credit cards	One year
• Pawn or buy property	Six months

Inquiries into the APS

The following table identifies a number of ways an inquiry can be made into the APS.

Inquiries based on...	*Minimum* information required
Name	• Name (**NAM**) • Date of Birth (**DOB**) or Age (**AGE**)
Serial Number	• Serial Number (**SER**) or Owner Applied Number (**OAN**) • Category Code (**CAT**) or Article Code (**ART**) or Brand (**BRA**) • Optional Information to Narrow Search Results • City, County Code (**CCC**)

Introduction

The **Automated Firearms System (AFS)** is a file of serialized firearm records. It includes law enforcement status records and historical records.

Law Enforcement Status Records

The following list identifies the types of information organized under law enforcement status in the AFS.

- Stolen
- Evidence
- Found/Safe Keeping
- Lost
- Institutional Registration
- Under Observation
- Retained for Official Use
- Destroyed

Historical Records

Historical records are files pertaining to firearms that are associated with a person. The following list identifies the firearm historical records available in the AFS.

- Buy or trade
- Consignment
- Dealer's Record of Sale (DROS)
- Serial number assigned
- Serial number restored
- License to carry concealed weapon (CCW)
- Pawn
- Voluntary registration
- Sold at auction
- Assault weapon registration

Types of Firearms Included in the AFS

There are a number of different types of firearms included in the AFS.

- Cannon
- Submachine
- Rifle/shotgun
- Grenade
- Rocket
- Machine gun
- Mortar
- Pistol
- Rifle
- Shotgun
- Tear gas weapon
- Silencer
- All others

Categories of Firearms Included in the AFS

Firearms are also recorded by category in the AFS. The following list identifies categories.

- Automatic
- Bolt action
- Carbine
- Derringer
- Double barrel
- Flare gun
- Gas/air gun
- Flintlock
- Semiauto
- Jet propulsion
- Blank pistol
- Lever action
- Machine gun
- Launcher
- Over/under
- Pump action
- Antique
- Revolver
- Single shot
- Recoilless
- Percussion
- Three barrels
- Four or more barrels

Inquiries into the AFS

The following table identifies the information that is required to gain access to both the law enforcement records and the historical records in the AFS.

Inquiries into...	*Minimum* information required
Law enforcement status records	• Serial Number (**SER**) only or • Serial Number (**SER**) • Make (**MAK**) or Caliber (**CAL**)
Historical records	• Name (**NAM**) • Date of birth (**DOB**) or Age (**AGE**) or • Serial Number (**SER**) only or • Serial Number (**SER**) • Make (**MAK**) or Caliber (**CAL**)

MENTAL HEALTH FIREARMS PROHIBITION SYSTEM (MHFPS)

Introduction

The **Mental Health Firearms Prohibition System (MHFPS)** is an *inquiry-only* database. The MHFPS contains information on persons prohibited from owning or possessing firearms.

Prohibitions

The prohibitions noted under the MHFPS may have resulted from a:

- Voluntary or involuntary commitment to a mental health facility. *(Welfare and Institutions Code Section 5150)*
- Report from the person's attending psychotherapist that the individual has made a serious threat of physical violence against reasonably identifiable victim(s)
- Superior court judgment concerning mental competency

Inquiries into the MHFPS

Access and use of information in the MHFPS are restricted by *Welfare and Institutions Code Sections 8100 through 8105*.

Agencies currently authorized to receive criminal history information may access the system only when conducting a criminal investigation which involves the acquisition, carrying, or possession of firearms.

Learning Need

Peace officers must know the requirements for access and entry into the appropriate Department of Justice information systems and databases available on the CLETS network to perform their duties for their safety and the safety of others.

Criminal Justice Information System (CJIS) [36.02.1]

The CJIS network is a computerized system containing records that are of interest to the criminal justice community maintained by the California Department of Justice in Sacramento.

Minimum Information Requirements [36.02.12]

There is some standard information that is required for each type of inquiry made. There is specific information needed for each specific type of inquiry.

Introduction

To help you review and apply the material covered in this chapter, a selection of learning activities has been included. No answers are provided. However, by referring to the appropriate text, you should be able to prepare a response.

Activity Questions

1. A six-year-old San Diego boy has been kidnapped by his father's ex-girlfriend. What system or systems might be used to alert law enforcement professionals in California?

2. Continuing the scenario of question 1: What systems could investigating officers use to obtain background information regarding the suspect? What would be the minimum information that would be needed to access those systems?

Activity Questions (Continued)

3. A ride share driver has brought an elderly woman to your district law enforcement station. The driver said he found her wandering down the street by a local park. The well-dressed woman had no ID and could not remember her name or where she lived. She appears tired and says that she is hungry. What information systems could you access to investigate the woman's identity? What is the minimum information you will need to make these inquiries?

4. How does the information contained in the WPS compare with the type of information contained in the CHS?

Activity Questions (Continued)

5. List all of the types of information that would be accessible from CJIS using only the information provided on your driver license and any other form of identification or documentation that you carry regularly in your wallet or purse. What systems could be accessed to obtain each piece of information?

6. You have stopped a man who was riding a bicycle at night without using any lights. When you ask the man for identification, he opens his backpack to reveal a number of tools that are often used as burglary tools. The man provides a California Identification Card. Based on the information you have, what systems can you access from CJIS? What type of information about the man can you obtain from each system?

Activity Questions (Continued)

7. List the systems you would access and the minimum information you would need to conduct inquiries based on the following circumstances.

Circumstance	**CJIS System(s)**	**Minimum Information Required**
To determine whether a subject has any outstanding warrants		
To find out the probation/parole status of a suspect		
To determine the owner of a handgun found at the scene of a robbery		

Chapter 3
Department of Motor Vehicles Information System

OVERVIEW

Learning Need

Peace officers must know the requirements for access and entry into the appropriate Department of Motor Vehicles information systems and databases available on the CLETS network to perform their duties, and to ensure their safety and the safety of others.

Learning Objectives

The chart below identifies the student learning objectives for this chapter.

After completing study of this chapter, the student will be able to:	Objective ID
• Identify systems and databases available from the Department of Motor Vehicles Information System and the types of information provided	36.03.1
• Recognize the minimum information required for generating an inquiry into each of the DMV databases	36.03.5

In This Chapter

This chapter focuses on the DMV information accessible through the CLETS network. Refer to the chart below for specific topics.

Topic	See Page
Department of Motor Vehicles Systems/Databases	3-3
Vehicle/Vessel Registration Database (VVRD)	3-7
Chapter Synopsis	3-12
Workbook Learning Activities	3-13

DEPARTMENT OF MOTOR VEHICLES SYSTEMS/DATABASES

Introduction

The California Department of Motor Vehicles (DMV) maintains a number of databases that are accessible to authorized users through the CLETS network.

DMV Databases

Access to the DMV files is intended strictly for the purpose of enforcing the law. *(Vehicle Code Section 1808.47)*

The following automated databases are maintained by the DMV:

- Driver License/Identification Card
- Vehicle/Vessel Registration
- Parking/Toll Violation
- Occupational Licensing
- International Registration Plan

Driver License/Identification Card Database

The **Driver License/Identification Card Database** maintains automated records of all:

- California licensed drivers
- Unlicensed drivers who have been arrested and/or have received citations
- Those persons who have been issued a California Identification Card

Available Information

The following table identifies further information regarding the Driver's License/Identification Card database.

Information included	Description
Basic record	• Information such as the driver's: - License or identification card number - Date of birth - Name - Address - Aliases and monikers
Status of driving privilege	• License issuance information • Restriction information • Year of license expiration • Information on replication • Mailing date of new identification cards
Legal history	• Description of the major legal actions taken against the driver • Reinstatement information
Abstract of conviction	• Violation date • Conviction date • Statute and section violated • Docket number • Court • Court action and final court disposition • Vehicle license number

Available Information (Continued)

Information included	Description
Description of the subject's legal actions	• Including cases in which subject failed to appear before the court
Record of subject's accidents	• Dates • Locations • Vehicle license number • Whether cited • Accident report number • Financial responsibility case number
Endorsements and certificates	• Type of endorsement or certificate • Issue date • Expiration date • Applications other than original or renewal • Type of application • Office of issue
Identifying information	• Physical description

Inquiries

The following table identifies the information required to make an inquiry into the Driver's License/Identification Card database.

Inquiries based on...	Required information	Optional information to narrow search results
Name	• Last name • First name	• Middle initial • Date of birth or age • City and first three numbers of the person's street address
Other	• Driver's license number	
	• Identification card number	

NOTE: For name inquiries, the last name is matched by a Soundex system. No such system is used for spelling the first name. Because of this, officers should take care to spell the individual's first name exactly as it appears on the driver's license or identification card.

NOTE: The driver license number and identification card number appear as a single alpha character followed by seven (7) numbers, (e.g., A1234567).

NOTE: If a person is cited or arrested for a Vehicle Code violation and/or involved in an accident and he or she has no California driver license or ID card issued to him or her, an unverified record is created starting with the letter "X" followed by seven (7) numbers.

VEHICLE/VESSEL REGISTRATION DATABASE (VVRD)

Introduction

The DMV maintains an ongoing **Vehicle/Vessel Registration database (VVRD)** which provides a record of ownership. This file includes all vehicles and vessels registered, or with planned non-operation status.

Records are updated by renewals, changes of address, or transfers. Parking, owner responsibility citations, and delinquent property taxes on vessels can temporarily become part of these records.

Available Information

The Vehicle/Vessel Registration database contains:

- License plate number of all vehicles or vessel CF numbers
- Descriptions of the vehicle or vessel
- Name and address of the registered owner, lessee, lessor
- If present, the legal owner
- The status of the record
- Owner-as-of-information (prior, pending, and current owner information to determine the owner of vehicle "*as of*" a specified date and time)

DOJ Stop, Restraint, and Referral

When a stolen vehicle, felony vehicle, or stolen vehicle part entry is accepted by the CJIS SVS the corresponding DMV vehicle/vessel record is flagged. This is also true for a stolen boat or boat parts when entry is accepted by the CJIS ABS.

Flags on a DMV Vehicle/Vessel Registration record are intended to prevent the registration of stolen vehicles and boats. Officers who encounter *STOP*, *RESTRAINT*, or *REFERRAL* flags on any record should contact the Department of Justice Stolen Vehicle Unit.

Inquiries

The following table identifies the information that is required to make an inquiry into the Vehicle/Vessel Registration database.

Inquiries regarding...	Required information	Optional information to narrow search results
Vehicles	• Vehicle license number *and/or* • Vehicle identification number • Name *and/or* • Company	• Name (last and first name) *or* • Company name (first 35 characters of the name) • City and first three numbers of the person's address • Make and year of vehicle
Handicap placards	• Placard number, or • Name (last name and first name)	• City and first three numbers of the person's street address
Vessels	• Hull or identification number *and/or* • Boat registration number • Name *and/or* • Company	• Name (last and first name) *or* • Company name (first 35 characters of the name) • City and first three numbers of the person's street address • Make and year of vehicle

Parking/Toll Violation Database

The DMV **Parking/Toll Violation database** contains a record of all outstanding parking and toll violations. (Delinquent toll evasion violations are stored as parking violations.)

Vehicle Code Section

Vehicle Code Sections 40200-40230 require the DMV to refuse registration renewal on a vehicle when an agency or court has placed an unpaid parking violation "hold" on the vehicle registration record. The hold remains on the record until payment or proof of payment is received.

Vehicle Code Section 22651(i) allows law enforcement agencies to impound certain vehicles with unpaid parking citations. Vehicles cannot be towed or booted for delinquent toll evasion violations.

Available Information

Information included in the Parking/Toll Violation database includes:

- A brief description of the vehicle
- The registered owner's name and address
- A listing of parking/toll violations applied to the vehicle
- Handicap placard information

A maximum of 75 violations for each vehicle record are furnished.

Inquiries

Inquiries can be made into the Parking/Toll Violation database by using the:

- Vehicle License Number (VLN)
- Vehicle Identification Number (VIN)

Occupational Licensing Database

The DMV has the responsibility of maintaining a complete **Occupational Licensing Database** of every person or business who holds an occupational license.

Available Information

The following table identifies the information that is maintained in the DMV Occupational Licensing Database.

Information included	Description
Firm file	• Contains the organizations licensed by the DMV to operate certain specified types of businesses in the state (e.g., auto dealers, driving schools, vessel agents, etc.)
Individual file	• Contains the names of persons licensed by the agency either as separate entities or connected with the organizations stored in the Firm File (e.g., salesperson, driving instructors, etc.)

Inquiries

Inquiries into the Occupational Licensing Database can be made by using the:

- Dealer license plate number
- Firm
- Individual record identifier number

International Registration Plan Database

The DMV maintains an automated record of companies that register fleets of commercial vehicles.

The **International Registration Plan** is a licensing and reciprocity agreement between 47 jurisdictions that sets forth the procedures for registration and operation of vehicles that travel in two or more jurisdictions. Carriers may be based in or outside California.

The International Registration Plan requires the fleet owner to establish a “base jurisdiction” when registering the vehicles. A base jurisdiction can be any jurisdiction provided it is where:

- The registrant has an established place of business
- Mileage is accrued by the fleet
- Operational records of the fleet are maintained or can be available

Learning Need

Peace officers must know the requirements for access and entry into the appropriate Department of Motor Vehicles information systems and databases available on the CLETS network to perform their duties, and to ensure their safety and the safety of others.

Department of Motor Vehicles (DMV) [36.03.1, 36.03.5]

The DMV maintains a number of databases that are accessible to authorized users through the CLETS network. Specific information is required for inquiries into the different databases.

Introduction

To help you review and apply the material covered in this chapter, a selection of learning activities has been included. No answers are provided. However, by referring to the appropriate text, you should be able to prepare a response.

Activity Questions

1. A peace officer responds to a call of an abandoned vehicle in a downtown parking lot. The lot attendant tells the officer that the car, a late model sports car, has been left in the parking space for over a week. The car has California license plates. In what DMV database(s) might the officer search for information regarding the vehicle? What type of information might the officer receive in response?

2. Continuing the scenario of Question 1: Besides what is available from the DMV, what other systems or databases might provide the officer with information? What type of information might the officer receive from these other system(s) or database(s)?

Activity Questions (Continued)

3. List all the types of information accessible by using only a vehicle license number. Consider both the CJIS and the DMV systems and databases when writing your answer.

Supplementary Material

In This Section

Refer to the following table for specific reference documents included in this section.

Topic	See Page
Acronyms/Abbreviations	S-2
CLETS Network Overview Table	S-7
CLETS Network Diagram	S-11

A

ABS	Automated Boat System
ACHS	Automated Criminal History System
AFS	Automated Firearms System
APB	All Points Bulletin
APS	Automated Property System
ARE	Area
ART	Article Number

B

BHN	Boat Hull Number
BOLO	Be-On-the-Look-Out
BPS	Body Part Status
BRA	Brand

C

CAL	Caliber
CARPOS	California Restraining and Protective Order System
CAT	Category
CCC	City, County Code
CCW	Carry Concealed Weapon
CDCR	California Department of Corrections and Rehabilitation
CHS	Criminal History System
CII	Criminal Identification and Information Number
CJIS	Criminal Justice Information System
CLETS	California Law Enforcement Telecommunications System
CNT	County or Region
CORI	Criminal Offender Record Information
CPIC	Canadian Police Information Center

D

DCH	Dental Characteristics
DJJ	California Department of Juvenile Justice
DLC	Day of Last Contact
DLN	Driver License Number
DMV	Department of Motor Vehicles
DOB	Date of Birth
DOC	Department of Corrections Number
DROS	Dealer’s Record of Sale

E

EDD	Estimated Date of Death
ENG	Engine Number
EYE	Eye Color

F

FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FCN	File Control Number

G

H

HAI	Hair color
HGT	Height

I

ID	Identification

J

K

L

LIC	License Plate Number

M

MAK	Make
MCHS	Manual Criminal History System
MDT	Mobile Digital Terminal
MHFPS	Mental Health Firearms Prohibition System
MNE	Terminal Mnemonic
MNI	Master Name Index
MNU	Miscellaneous Identification Number
MUPS	Missing/Unidentified Persons System

N

NAM	Name
NCIC	National Crime Information Center
NLETS	National Law Enforcement Telecommunications System

O

OAN	Owner Applied Number
OCA	Originating Agency Case Number
OLN	Operator’s License Number
ORI	Originating Agency Identifier

P

PRCS	Post Release Community Supervision

Q

R

RAC	Race
REG	Registration Number

S

SAR	Sex and Arson Registration
SER	Serial Number
SMT	Scars/Marks/Tattoos
SOC	Social Security Number
SRF	Supervised Release File
SVS	Stolen Vehicles System

T

TYP	Type

U

V

VCIN	Violent Crime Information Network
VCM	Vehicle Make
VCO	Vehicle Color
VIN	Vehicle Identification Number
VLN	Vehicle License Number

W

WGT	Weight
WPS	Wanted Persons System

X

Y

Z

Introduction

The following table identifies the numerous systems that are accessible through the CLETS network.

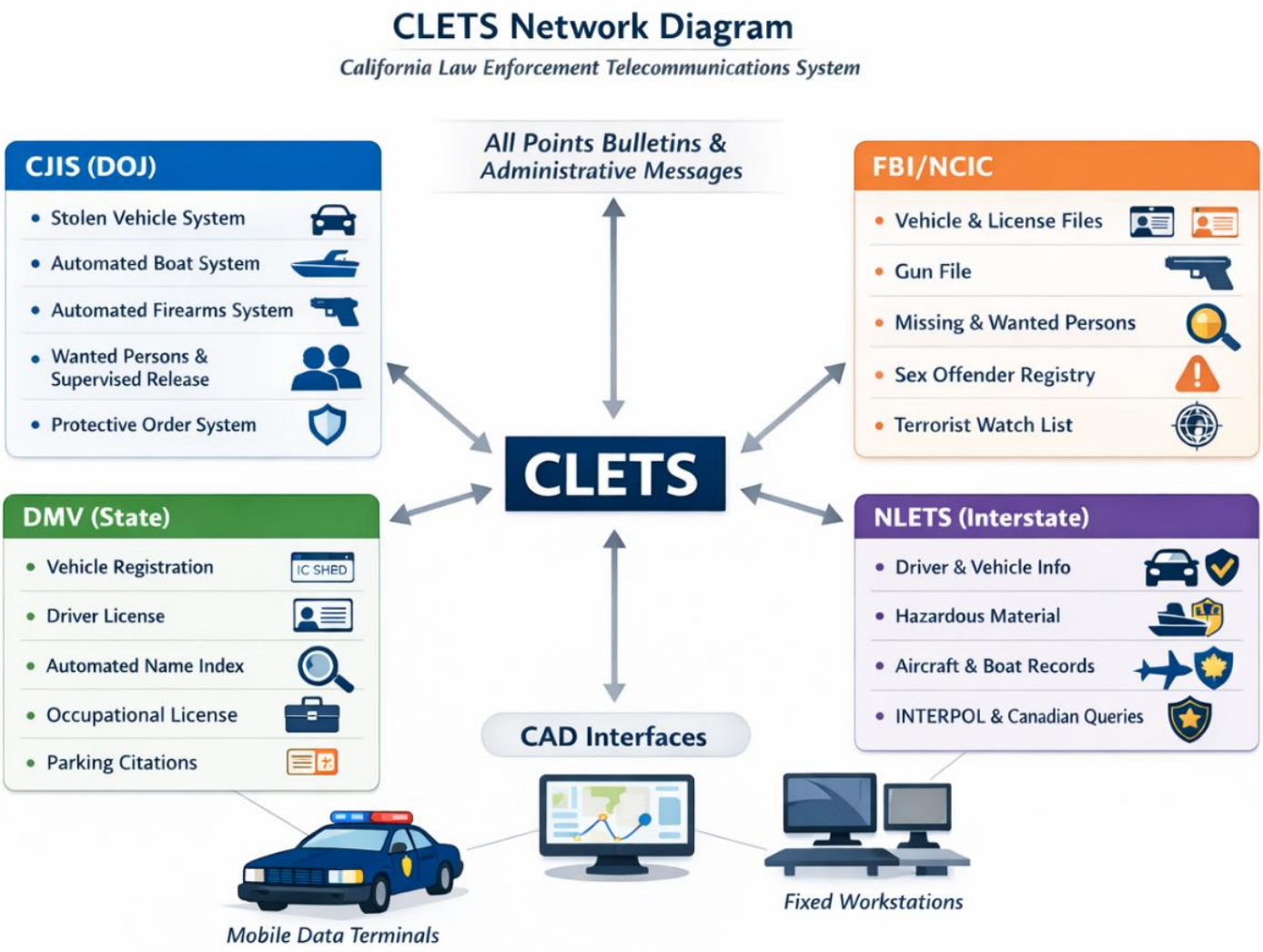
Network	System	Subsystem/File/Database
CLETS (California Law Enforcement Telecommunications System)	**CJIS** (Criminal Justice Information System)	**CHS** (Criminal History System)
		WPS (Wanted Persons System)
		SRF (Supervised Release File)
		CARPOS (California Restraining and Protective Order System)
		MUPS (Missing/Unidentified Persons System)
		VCIN/SAR (Violent Crimes Information Network/Sex and Arson Registration)
		SVS (Stolen Vehicle System)
		ABS (Automated Boat System)
		APS (Automated Property System)
		AFS (Automated Firearms System)
		MHFPS (Mental Health Firearms Prohibition System)

Network	System	Subsystem/File/Database
CLETS (Continued)	**DMV** (Department of Motor Vehicles)	Driver License/Identification Card
		Vehicle/Vessel Registration
		Parking/Toll Violation
		Occupational Licensing
	NCIC	Interstate Identification Index
		Wanted Person File
		Deported Felon File
		Protection Order File
		Missing Person File
		Unidentified Person File
		Vehicle File
		License Plate File
		Boat File
		Gun File
		Article File
		Securities File

Network	System	Subsystem/File/Database
CLETS (Continued)	**NCIC** (Continued)	Foreign Fugitive File
		US Secret Service File
		Bureau of Alcohol, Tobacco, and Firearms Violent Felon File
		Violent Gang and Terrorist Organizations File
	NLETS (National Law Enforcement Telecommuni-cations System)	Vehicle registration
		Driver License
		Criminal History Record Information
		Hazardous Material File
		FAA Aircraft Registration System
		FAA Aircraft Tracking System
		National Center for Missing and Exploited Children
		National Insurance Crime Bureau

Network	System	Subsystem/File/Database	
CLETS (Continued)	**NLETS** (Continued)		
		CPIC	Administrative Messages

		(Canadian Police Information Center)	Persons Files
			Stolen Vehicle File
			Vehicle Registration File
			Driver License File
			Article File
			Boat File
			Gun File
			Securities File
			Criminal History File


CLETS Network Diagram
California Law Enforcement Telecommunications System
CJIS (DOJ)
Stolen Vehicle System
Automated Boat System
Automated Firearms System
Wanted Persons & Supervised Release
Protective Order System
All Points Bulletins & Administrative Messages
FBI/NCIC
Vehicle & License Files
Gun File
Missing & Wanted Persons
Sex Offender Registry
Terrorist Watch List
CLETS
DMV (State)
Vehicle Registration
IC SHED
Driver License
Automated Name Index
Occupational License
Parking Citations
NLETS (Interstate)
Driver & Vehicle Info
Hazardous Material
Aircraft & Boat Records
INTERPOL & Canadian Queries
CAD Interfaces
Mobile Data Terminals
Fixed Workstations

Glossary

Introduction

The key vocabulary terms for Learning Domain 36: Information Systems are listed below with the definitions as they apply to this workbook.

Automated Boat System (ABS)

A component of the CJIS; database containing records of watercrafts that have been reported stolen, lost, repossessed, and stored

All-Points Bulletin (APB)

An administrative message that is distributed or received via CLETS to law enforcement agencies in the state

Access

To gain entry to, instruct, or communicate with the resources of a computer, a computer system, or a computer network

Automated Firearms System (AFS)

A component of the CJIS; a file of serialized firearm records

Automated Property System (APS)

A component of the CJIS; a file of serialized property records

Administrative Messages

A component of CLETS used to send information from point to point in free text (i.e., All Points Bulletin (APB), Be-On-The-Look-Out bulletin (BOLO))

BOLO

Be-On-the-Look-Out bulletin regarding missing or wanted persons

California Restraining and Protective Order System (CARPOS)

A component of the CJIS; identifies restraining protective orders entered by law enforcement agencies

Criminal History System (CHS)

A component of the CJIS; contains criminal history information that is available to criminal justice agencies on a “right-to-know” and a “need-to-know” basis

CII

Criminal Identification and Information number

Criminal Justice Information System (CJIS)

Criminal Justice Information System; a computerized system containing records that are of interest to the criminal justice community; maintained by the California Department of Justice network

California Law Enforcement Telecommunications System (CLETS)

A computer system that provides all law enforcement user agencies with the capability of obtaining information directly from federal and state computerized information files

Confirmation

Checking with the originating agency to establish if the person or property is still wanted and is probably the same as the person or property being inquired about

Criminal Offender Record Information (CORI)

Criminal Offender Record Information; records and data compiled by criminal justice agencies for the purposes of identifying criminal offenders

Data

A representation of organized information, knowledge, facts, or concepts collected for a specific purpose

Database

A collection of like or related data

Driver License/Identification Card Database

A component of the DMV information system; contains automated records of all California licensed drivers, unlicensed drivers who have been arrested and/or have received citations, and those persons who have been issued a California Identification Card

Free Text

An unformatted statement or message in common language

International Registration Plan (IRP)

A licensing and reciprocity agreement between 47 jurisdictions that sets forth the procedures for registration and operation of vehicles that travel in two or more jurisdictions

Mental Health Firearms Prohibition System (MHFPS)

A component of the CJIS; contains information on persons prohibited from owning or possessing firearms

Missing & Unidentified Person System (MUPS)

A component of the CJIS; a file of records which catalogs reports of missing or unidentified persons according to a variety of physical and dental characteristics

Need-to-Know

The compelling need to obtain CORI in order to execute official responsibilities

Occupational Licensing Database

A component of the DMV information system; a record of every person or business who holds an occupational license

Owner Applied Number (OAN)

Any number permanently affixed to an item by the owner of the item

Parking/Toll Violation Database

A component of the DMV information system; a record of all outstanding parking and toll violations

Pointer System

A system that provides a brief indicator showing that a record exists and identifies the agency or source that maintains the complete information

Rap Sheet

Summaries of criminal history records

Right-to-Know

The right or authority to obtain CORI pursuant to a court order, statutory law, or case law

Sex and Arson Registration (SAR)

One increment of the VCIN system; statewide files on convicted persons required to register as sex offenders pursuant to *Penal Code Section 290* or arson offenders pursuant to *Penal Code Section 457.1*

Supervised Release File (SRF)

A component of the CJIS; contains brief but informative probation and parole indexes to the supervising agency's more complete records. The SRF also allows officers to send information about an encounter with a subject

Stolen Vehicle System (SVS)

A component of the CJIS; database containing records related to vehicles, license plates, and vehicle parts

Terminal Mnemonic (MNE)

The four-character address (terminal name) assigned by the DOJ/CLETS

Violent Crime Information Network (VCIN)

Database administered by the state Department of Justice and accessible through CJIS; contains consolidated information from a number of current DOJ systems

Vehicle/Vessel Registration Database (VVRD)

A component of the DMV information system; provides a record of ownership of all vehicles and vessels registered, or with planned non-operation status

Wanted Persons System (WPS)

A component of the CJIS; a file of records pertaining to wanted fugitives and arrest warrants