OFFICE OF THE CHIEF OF POLICE

SPECIAL ORDER NO. January 25, 2023

APPROVED BY THE BOARD OF POLICE COMMISSIONERS ON January 24, 2023

SUBJECT: **ELECTRONIC SURVEILLANCE EQUIPMENT – DEFINED, AND VARIOUS RELATED MANUAL SECTIONS – REVISED**

PURPOSE: This Order revises various Department Manual sections regarding emerging technologies and software that can be utilized to track the movements of a person or object. Assembly Bill 904, which was signed into law on September 11, 2020, specifically revised the definition of "tracking device" to include software and consequently applies to the provisions for obtaining a tracking search warrant.

PROCEDURE: Department Manual Sections 3/568.05 through 3/568.50, and 4/742.15, have been revised. The revised Manual sections are attached with the revisions indicated in italics.

AMENDMENTS: This Order amends Department Manual Sections 3/568.05 through 3/568.50; and, Section 4/742.15.

AUDIT RESPONSIBILITY: The Commanding Officer, Audit Division, shall review this directive and determine whether an audit or inspection shall be conducted in accordance with Department Manual Section 0/080.30.

MICHEL R. MOORE
Chief of Police

Attachments

DISTRIBUTION "D"

742.15 MANDATORY COMPLIANCE WITH ELECTRONIC COMMUNICATION PRIVACY ACT. The provisions and requirements of the California "Electronic Communication Privacy Act" (*California* Penal Code Sections 1534, 1546, 1546.1 and 1546.2) governs access to and retrieval of evidence from service providers or digital devices (computer forensics). Digital devices include, but are not limited to: computers, cellular telephones, hard drives, floppy disks, thumb drives, memory cards, MP3 players, digital video recorders (DVR), *any device or software that permits the tracking of the movement of a person or object, and* any items capable of storing digital data. **Failure to comply with the Electronic Communications Privacy Act may result in the suppression of evidence and/or civil liability.**

> ***Note:*** An electronic device does not include the magnetic strip on a driver's license or identification card issued by California or another state.

*Department Personnel shall ensure that t*he following key requirements *are met*:

- *Personnel shall adhere to the procedures outlined in Department Manual Section 1/140.15 when requesting the acquisition and use of certain systems and technologies.*
- Personnel *shall* have either a search warrant, wiretap order, or an order for a pen register or trap and trace device (or both) to compel production of or access *to* "electronic communication information" from a service provider;
- Personnel *shall have* either a search warrant, wiretap order, or an order for a pen register or trap and trace device (or both) to compel production of or access *to* "electronic device information" from a person or entity other than the "authorized possessor" of the device;

  Note: An authorized possessor is defined as the person who is in actual possession of an electronic device and who either owns the device or has the owner's permission to have possession of the device.

- Personnel may access electronic device information by means of physical interaction or electronic communication with the device, only where they have a search warrant, wiretap order, tracking device search warrant [pursuant to *California* Penal Code Sections 1524(a)(12) and 1534(b)] or order for a pen register or trap and trace device (or both);
- As exceptions to the warrant/order requirements, personnel may access electronic device information by way of direct manipulation or electronically connecting with the device:

  A. With specific consent from the authorized possessor of the device (Consent to Search, In House Form 11). Specific consent is defined as consent that is given directly to the government entity seeking information.

  Note: When a government entity is the intended recipient on an electronic communication, this satisfies "specific consent," even if the person making the communication does not have actual knowledge that he or she is communicating with the government.

B. With specific consent from the owner of the device, only when the device has been reported lost or stolen;
C. When they have a good faith belief that an "emergency" exists. "Emergency" under this section is limited to circumstances involving danger of death or serious physical injury to any person;

Note: When the electronic information is obtained due to an "emergency," Department personnel *shall*, within three **court** days of obtaining the information, file an application for a search warrant or court order.

D. If the device is seized from an authorized possessor of the device who is either on parole (under the supervision of the Department of Corrections and Rehabilitation) or a term of post release community supervision (under the supervision of County Probation);
E. If the device is seized from an authorized possessor of the device who is subject to an electronic device search as a clear and unambiguous condition of probation, mandatory supervision, or pretrial release; and,

Note: Personnel *shall* verify the existence of a specific electronic device search provision **prior to** accessing electronic device information based on this exception.

F. Where personnel are accessing information concerning the location or telephone number of the device specifically in order to respond to an emergency 9-1-1 call from that device.

- Personnel *shall* adhere to the following when applying for warrants under this section:

A. All search warrants shall describe with particularity, the information to be seized, and must include, as appropriate and reasonable:

1. The time periods covered;
2. The target individuals or accounts;
3. The applications or services covered; and,
4. The types of information sought.

Note: In the case of a search warrant for access to electronic device information by means of physical interaction or electronic communication with the device, the court may determine that it is not appropriate to specify time periods, due to specific circumstances surrounding the investigation (including the nature of the device to be searched).

B. The warrant *shall disclose* that any information obtained through the warrant 's execution that is unrelated to the objective (outside the scope) of the warrant shall be sealed and not subject to further review, use, or disclosure, without a court order or to

comply with discovery required by *California* Penal Code *Sections 1*054.1 and 1054.7; and,

C. If the investigating officer seeks "electronic communications information" from a service provider, the warrant shall be accompanied by an order requiring the service provider to verify the authenticity of any electronic information produced.

- When a service provider *voluntarily* discloses electronic communication or subscriber information:

  A. Department personnel *shall* destroy the information within 90 days, unless:

     1. Department personnel receive specific consent from the sender or recipient of the information; or,
     2. Department personnel obtain a court order authorizing retention of the information; or,
     3. Department personnel reasonably believe the information is related to a child pornography crime and the information is stored in a multi-agency database and retained as evidence of such case(s) or related crime(s); or,
     4. The service provider or subscriber is, or discloses the information to, a federal, state or local prison, jail or juvenile detention facility, and ALL participants to the electronic communication were told, prior to the communication, that the service provider may disclose the information to the government entity.

- Investigating officers *shall* serve *notice* to the identified target of the search warrant or target of the emergency access to the device. This notice *shall*:

  A. Inform the target that information about them has been compelled or requested;

     Note: *Pursuant to Assembly Bill No. 904 "No later than 10 calendar days after the use of the tracking device has ended, the officer who executed the tracking device warrant shall notify the person who was tracked or whose property was tracked." Notification is pursuant to 1546.2(a) P.C.*

  B. State, with reasonable specificity, the nature of the investigation regarding the obtained information;
  C. Include a copy of the search warrant, or, in the case of an emergency, a written statement setting forth facts giving rise to the emergency;
  D. *M*ade contemporaneous to the execution of the warrant. If the electronic information was obtained as the result of an emergency, notice shall be served within three court days after obtaining the electronic information;

     Note: Service shall be affected by personal service, or delivered by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective.

E. *Be communicated by the i*nvestigating officers are required to serve notice to the Department of Justice within three days of the execution of the search warrant when the target of the search warrant is not known; and,

Department personnel may seek to delay the required notice, and prevent any party from notifying the target that information has been sought:

A. Pursuant to a request included in the warrant affidavit;
B. Where the court determines there is reason to believe that notification may have an "adverse result";
C. *For* up to 90 days *by the court*, with court-issued extensions available.

When the extension period expires, the affiant must serve notice to the target, and the notice shall:

A. Inform the target that information about them has been compelled or requested;
B. State, with reasonable specificity, the nature of the investigation regarding the obtained information; and,
C. Include a copy of the search warrant, or, in the case of an emergency – a written statement setting forth facts giving rise to the emergency, and include a copy of the electronic information obtained or a summary of it (include the number and type of records, date/time records created, and statement of grounds for court order delay in notification).

Note: The California Electronic Communications Privacy Act does not change the authority of the Department to compel employees authorized to possess Department-issued electronic devices to return such devices to the Department.

DEPARTMENT MANUAL
VOLUME III
Revised by Special Order No. 5 , 2023

568.05 ELECTRONIC SURVEILLANCE EQUIPMENT – DEFINED. Electronic surveillance equipment is *defined as equipment or software* used to detect, locate, observe, photograph, record, or intercept information about persons under Department investigation without their knowledge. *As such, all electronic surveillance equipment is subject to the provisions outlined in Department Manual Section 1/140.15 and personnel shall adhere thereto when acquiring or using electronic surveillance equipment while on duty.*

Electronic surveillance equipment is divided into two categories:

I. **Restricted Items.** Use of restricted electronic surveillance equipment requires authorization of a command or staff officer. Restricted items normally include all electronic surveillance equipment designed or adapted for concealed use. Included are items such as:

- Pen registers;
- Trap traces;
- Transmitters capable of being concealed in an automobile, room or telephone;
- Body transmitters;
- Induction coils;
- *Devices and software used for the purpose of tracking the movement of a person or object;*
- Receivers and recorders when used with hidden transmitters; *and,*
- Tracking or tailing devices and other non-visual equipment.

Note: With the exception of miniature *voice or video* recorders, on-duty employees shall not possess or use privately owned restricted electronic surveillance equipment. When used, privately owned miniature recorders are subject to the same authorization requirements as other restricted items.

II. **Discretionary Items.** Discretionary items are those items not specifically designed for concealed use, but which can be used in a concealed manner. When used for such purposes, discretionary items temporarily become restricted items of electronic surveillance equipment, and, as such, their use is controlled. Discretionary items include tape recorders, mini-recorders, hand-held radio receivers, T.V. cameras and video recorders, night-*vision* devices, repeaters and cameras.

Note: A surveillance van is considered a discretionary item unless it is used in conjunction with a camera and lens at which time it is considered a restricted item.

Equipment Storage. Restricted electronic surveillance equipment shall generally be stored in a secured location within a Department facility. However, if it is required by the nature of the investigation, equipment used by specialized units in certain divisions (e.g., Gang and Narcotics Division, *Detective Support and* Vice Division, Major Crimes *Division*, Professional Standards Bureau) may be stored in *Department* vehicles, as long as it remains under the command and control of the investigating officer and as long as it remains in good working order.

Provide Security. All employees using electronic surveillance equipment shall provide security for the equipment while it is in their possession.

Time Restrictions. Restricted electronic surveillance equipment shall generally be used for a period of time not to exceed 30 days. However, equipment used in investigations by specialized units in certain divisions (e.g., Gang and Narcotics Division, *Detective Support and* Vice Division, Major Crimes Division, Professional Standards Bureau) may be used for the duration of the investigation, in excess of 30 days, provided that the equipment is accounted for, remains in good working order and prior approval is obtained.

Should the investigation exceed the 30-day time limit, the investigating officer shall complete an Employee's Report, Form 15.07.00, documenting the reasons for the additional time required and the condition of the equipment. The Employee's Report shall be completed and approved prior to the expiration of the due date. The investigating officer shall forward the Employee's Report to *their* commanding officer for approval.

Investigating Officer's Responsibilities. *Investigating officers shall* ensure that the equipment is safely returned to the assigned unit as soon as possible after the equipment's usage.

Commanding Officer's Responsibilities. The divisional *or* Area commanding officer *shall* review and, if appropriate, approve the investigating officer's written request for the extended use of the equipment for each additional 60-day period. Once approved, the Employee's Report shall be forwarded to the Department entity originally furnishing the equipment so that it may be filed with the original *Authorization* to Use *Restricted* Electronic *Surveillance* Equipment, Form 12.41.00.

568.10 REQUESTS FOR USE OF RESTRICTED ELECTRONIC SURVEILLANCE EQUIPMENT. The following procedure shall be followed for every use of restricted electronic surveillance equipment.

Restricted Electronic Surveillance Equipment Policy. Investigating officers who use restricted surveillance equipment shall comply with all current State and Federal Laws, *the Department's Core Values and tenets of procedural justice.*

Obtain Authorization. Employees shall obtain proper authorization prior to using restricted electronic surveillance equipment *(e.g., authorization from a command or staff officer, an approved Authorization to Use Restricted Electronic Surveillance Equipment, Form 12.41.00, a warrant, and any policy specific to the equipment item).*

Complete Training. Prior to using electronic surveillance equipment, employees shall satisfactorily complete *any* required training, *if applicable.*

Investigating Officer's *Responsibilities.* Investigating officers who require the use of restricted surveillance equipment shall complete the top portion of an Authorization to Use Restricted Electronic Surveillance Equipment, Form 12.41.00, and submit the form to a supervisor for approval.

The investigating officer requesting extended use of the restricted electronic surveillance equipment shall:

- Include the request to use the restricted equipment for an extended period of time for 30 days *not to exceed a maximum extension of 60 days or as authorized by a magistrate*; and,
- Include a notation as to the method and location of storage (e.g., locker, secured desk) when restricted equipment is not *in use*.

Upon approval by a supervisor and a *c*aptain or above *Form 12.41.00* shall be submitted to the concerned equipment coordinator or Technical Investigation Division (TID) Electronics *Unit* personnel for equipment issuance. Daily usage of the restricted electronic surveillance equipment shall be documented on the Restricted Electronic Surveillance Equipment Monthly Usage Log, Form 12.41.01. The log shall be completed in the following manner:

- Entries shall be completed daily;
- Each entry shall be reviewed and signed by the supervisor of the concerned investigative unit; and,
- Upon completion of the investigation and the usage of the restricted electronic surveillance equipment, attach the completed log with *Form 12.41.00* and submit the completed forms to their supervisor for review.

The use of restricted electronic surveillance equipment does not always require the use of *Form 12.41.00. The form* is only required if the equipment is used to breech a person's reasonable expectation of privacy or is requested by the concerned commanding officer. Should the completion of *Form 12.41.00* be required, *the completed and approved form*, shall be submitted to the concerned equipment coordinator, the Technical Investigation Division (TID) Electronics *Unit,* or the relevant Department entity issuing the equipment.

> **Note:** When the investigation is of a sensitive nature, only the shaded items *on the form* are required to be completed.

Supervisor's *Responsibilities.* Supervisors reviewing *Form 12.41.00*, shall be responsible for:

- Reviewing the *form* and discuss*ing* the intended use of the equipment with the investigating officer(s);
- Pre-approving the *form*, and ensuring it is submitted to the concerned *c*aptain or above for approval; and,
- Upon completion of the investigation and use of the surveillance equipment, review*ing* *Form 12.41.01 and Form 12.41.00* and ensur*ing* the forms are forwarded to the concerned commanding officer.

Commanding Officer's Responsibilities. In addition to established responsibilities delineated in Department Manual Section 3/568.15, the commanding officer, of the rank of Captain or above shall:

- Review and approve *Form 12.41.00*; and,
- Ensure *Form 12.41.00 and Form 12.41.01* are forwarded to the concerned staff officer for review.

Note: When exigent circumstances exist, the Department *Operations Center* may be contacted for assistance in locating a staff officer. Bureau commanding officers or staff officers may grant telephonic authorization to use restricted electronic surveillance equipment when the circumstances of the situation do not allow for approval through normal channels. When telephonic approval is granted, the name of the approving bureau commanding officer or staff officer shall be printed on the *signature* line and the notation "telephonic" shall be placed next to the staff officer's name. *The officer/supervisor receiving the telephonic approval shall be the same person completing the form.*

568.15 REVIEW. Upon completion of the investigation and return of the equipment, the concerned commanding officer *and* a staff officer shall review the Authorization to Use Restricted Electronic Surveillance Equipment, Form 12.41.*00 and the Restricted Electronic Surveillance Equipment Monthly Usage Log, Form 12.41.01 for proper use and completion.*

Commanding Officer's Responsibilit*ies*. The commanding officer reviewing the restricted electronic surveillance equipment usage shall:

- Evaluate the equipment usage for its compliance with all the aspects of technical, legal, and procedural requirements for the use of restricted electronic surveillance equipment. Appropriate comments, if any, shall be made in the "After Action Evaluation" portion of the Form;
- Determine if the equipment was used as authorized. Whenever modifications or deviations are noted they shall be explained in the "After Action Evaluation";
- Ensure that serial numbers of any tape(s) used, and the date and time the equipment was returned to the issuing unit, are recorded in the appropriate sections of the "After Action Evaluation";
- Certify that a review of the equipment usage has been conducted by signing the "After Action Evaluation"; and,
- Cause *the* Form 12.41.00 to be delivered to the concerned staff officer for review.

Bureau Commanding Officer's or Staff Officer's Responsibilit*ies*. The bureau commanding *officer* or staff officer reviewing the use of restricted electronic surveillance equipment shall:

- Ensure that the concerned commanding officer has *the* Form 12.41.00 *and Form 12.41.01,* and *has* properly evaluated the technical, legal, and procedural aspects of the equipment usage;
- Document the review of the equipment usage by signing and dating *the* Form 12.41.00 *and Form 12.41.01*;

- Forward the completed Form 12.41.00 to the concerned equipment coordinator, Technical Investigation Division, *E*lectronics *Unit* or the relevant Department entity issuing the equipment; and,
- Notify the Chief of Police of any concerns and/or problems that arise from electronic surveillance equipment usage.

Chief of Detectives, Detective Bureau - Responsibilit*ies*. The Chief of Detectives, Detective Bureau, shall review all uses of restricted electronic surveillance equipment and shall be responsible for the following special duties relating to the use of such equipment:

- Maintain a confidential file of all approved Authorizations to Use Restricted Electronic Surveillance Equipment, Form 12.41.00;
- *Forward all Forms 12.41.00 and 12.41.01 to Innovation Management Division (IMD) for the Department's Comprehensive Technology Report (CTR) per Department Manual Section 1/140.15; and,*
- Evaluate equipment needs for maintenance, planned replacement, assessments of future technology and/or efficiency, and effectiveness of the Department equipment resources.

568.20 REQUESTS FOR ASSIGNMENT OF STORED ELECTRONIC INVESTIGATION EQUIPMENT. Requests for assignment of electronic investigation equipment stored at Technical Investigation Division shall be made by commanding officers on an Intradepartmental Correspondence, Form 15.02.00, in duplicate. Requests for assignment on a permanent basis shall be submitted through *the appropriate* channels to the Commanding Officer, Administrative Services Bureau. Requests for assignment on a temporary basis shall be submitted through *the appropriate* channels to the Commanding Officer, Technical Investigation Division. Electronic investigation equipment assigned on a temporary basis by Technical Investigation Division shall be returned upon completion of the assignment.

> **Note:** In an emergency, the Officer in Charge, Electronics Unit, Technical Investigation Division, may temporarily assign electronic investigation equipment, *with a signed Form 15.02.00 from the CO of the requesting entity,* pending the approval of the Commanding Officer, Technical Investigation Division.

568.40 CONTROL OF ELECTRONIC SURVEILLANCE EQUIPMENT. Control of electronic surveillance equipment is the responsibility of the commanding officers of the following organizational entities:

Unit to Which Equipment is Assigned – Responsibilities. The commanding officer of every unit which *receives* and uses electronic surveillance equipment shall be responsible for:

- Maintaining control over issuance of all electronic surveillance equipment assigned to the unit;
- Determining if *the* persons requesting the loan of electronic surveillance equipment are sufficiently qualified to properly use the equipment;

- Maintaining, in proper working order, all electronic surveillance equipment assigned to the unit; and,
- Ensuring that personnel have been properly trained prior to using electronic surveillance equipment. Such training shall encompass technical, legal, *procedural* and operational aspects of equipment usage.

  Note: The commanding officer of every unit which frequently uses or regularly maintains electronic surveillance equipment shall appoint a minimum of two officers to act as unit electronic surveillance equipment coordinators. Officers *to whom this duty is given* perform the*se* duties in addition to their regular assignment. Officers in this assignment shall have their days off and vacations scheduled so that one coordinator is always available during the unit's normal duty hours.

Unit Using Equipment – Responsibilities. The commanding officer of every unit using electronic surveillance equipment shall:

- Ensure that all officers using equipment are trained in the technical, legal, *procedural* and operational aspects of electronic surveillance equipment usage;
- Ensure that each use of restricted electronic surveillance equipment is documented by a completed and approved Authorization to Use Restricted Electronic Surveillance Equipment, Form 12.41.00;
- Ensure that the equipment, while it is in the possession of the unit, is adequately secured and that it is afforded care and maintenance to ensure its continued operation;
- Ensure that all equipment is returned to the unit assigned the item(s) as soon as possible; and,
- Ensure that whenever possible, all equipment installation and usage is completed in the presence of a supervisor.

Technical Investigation Division – Responsibilities. The Commanding Officer, Technical Investigation Division, shall be responsible for the following duties and functions related to all electronic surveillance equipment:

- Supervising the mechanical or technical aspects of all electronic surveillance equipment usage within the Department;
- Approving all replacement equipment for technical standards;
- Maintaining inventory records for all Department electronic surveillance equipment. Electronics *should be tracked in the Department's KITS system and an Equipment-Item Issue Control Card, Form 15.65.00;*
- Coordinating annual maintenance inspections and physical inventories conducted at the direction of each bureau commanding officer, and providing Technical Investigation Division assistance in such inspections and inventories;
- Reviewing all budget and grant requests for electronic surveillance equipment and all purchases of such equipment including component parts and attachments, to ensure Department-wide compatibility; and,

- Inspecting all newly-acquired equipment prior to its delivery to the requesting unit and inspecting all unserviceable equipment prior to its delivery to Supply Section for disposal.

Note: *Specialized Detective Divisions may be exempt from TID's oversight (e.g., Gang and Narcotics Division, Detective Support and Vice Division, Major Crimes Division, Professional Standards Bureau) pending approval from the entity's chain of command.*

568.45 SURVEILLANCE EQUIPMENT TRAINING RESPONSIBILITY. Training in the technical, legal, *procedural* and operational use of electronic surveillance equipment shall be the combined responsibility of the Commanding Officer, Training Division, and the commanding officer of any unit using electronic surveillance equipment.

Commanding Officer, Training Division – Responsibil*ities*. *The Commanding Officer, Training Division, shall be responsible for:*

- Developing a comprehensive training program to instruct members of this Department in the technical, legal, *procedural* and operational aspects of electronic surveillance equipment usage, *as applicable*; and,
- Incorporating electronic surveillance equipment training into Department schools for vice and narcotics officers, investigators, sergeants, lieutenants and captains.