CALIFORNIA HIGHWAY PATROL

GENERAL ORDER 10.26

JULY 2024

SECURITY CAMERA SYSTEM

1. GENERAL.

   a. Purpose. The purpose of this General Order (GO) is to establish standardized policies and procedures regarding the use of Security Camera Systems (SCS) at CHP facilities.

   b. Objective. The CHP desires to provide its employees with a workplace that is safe and secure. The implementation of SCS policies and procedures is intended to facilitate safe and secure work locations throughout the state. Utilizing cameras to survey public areas deters crime and assists in the protection and safety of CHP facilities and personnel. The SCS will also be used to monitor access to high-risk or restricted areas, such as evidence rooms. Security Camera Systems are maintained at the Area level; however, Emergency Operations and Safety Services (EOSS) section is the Office of Primary Interest.

2. DEFINITIONS.

   a. Security Camera System. A closed-circuit surveillance system. The purpose of the SCS is to increase security throughout the facility by utilizing video cameras to record data that can be viewed by departmental employees.

   b. Network. A group of computers that are linked in order to share resources or exchange information.

   c. Standalone. Standalone refers to a system that works independently and is not connected to a wider network.

   d. Camera. Any device that records images to be viewed or stored.

   e. Server. A computer that provides data storage for the SCS.

f. User. Any individual who is able to log into the SCS and view cameras or video recordings.

g. Administrator. Any user who is able to make changes to the SCS.

3. PROGRAM ADMINISTRATION. Security Camera Systems are used and managed by departmental personnel. These individuals are identified as users and are provided access to the software necessary to utilize the system. There are several different levels of control within the SCS.

a. Departmental Level. The EOSS Section is located within Protective Services Division. The EOSS Section personnel are the only users within the SCS who have administrative rights throughout the state. The EOSS Section shall work in conjunction with Information Technology Section (ITS) to ensure that access to the SCS software is only available to employees identified as appropriate users by EOSS Section.

b. Division Level. Each Division throughout the state shall have an assigned coordinator of the SCS which approves users within their respective Division.

c. Facility Level. Area offices or other CHP facilities which have a SCS installed, shall have at least one user who has access to their SCS. A CHP facility may have a standalone system; however, the policies contained within this GO still apply.

4. ACTIVATION. Users are responsible for ensuring the SCS operates and remains effective as a security tool. Cameras may be monitored live, or video recordings reviewed, for legitimate safety and security purposes which include, but are not limited to the following: high-risk areas, restricted access areas or locations (e.g., evidence rooms, cashier vaults), alarm or incident response, special events, and specific investigations authorized by an appropriate Area or section commander with articulable justification.

a. Audits. To ensure the system is secure, it is necessary for ITS to ensure that only approved users have access to the SCS.

(1) Transfers/Retirements. When users are no longer assigned to a position where they need access to the camera system, the command shall notify EOSS so their user account can be locked or removed by ITS.

b. Review. While accessing the SCS, the review process shall not focus on an individual employee, absent justification. When reviewing a video, supervisors and

managers are reminded to remain focused on the incident in question. Reviews are not intended for the purpose of identifying policy violations when no allegation of misconduct exists. If the need arises to view video to identify policy violations, Division commander approval shall be obtained prior to viewing the video.

c. Investigations. The discovery of any potential employee misconduct during the review of SCS recordings shall be handled in accordance with the policies outlined in Highway Patrol Manual (HPM) 10.2, Internal Investigations Manual, Chapter 5, Investigative Procedures. Video recordings shall be exported by the respective user for that Area, then provided to the commander before being distributed to the investigating personnel.

d. Ownership. Digital media obtained from the SCS is considered CHP property and shall only be used for safety and security purposes, for administrative or criminal investigations, or other purposes specified within this GO. Information obtained from security cameras is considered confidential and must be handled with the appropriate level of security to protect unauthorized access, alteration, or disclosure.

(1) Copies. All employees requesting copies of video recordings for review/release purposes, authorized by this GO, shall complete a memorandum, and submit the document to a supervisor for approval. Personal computer equipment and software programs shall not be utilized when making copies of video recordings. All recordings are the property of the Department, the copying of recordings by CHP personnel for unauthorized/personal use is prohibited except as otherwise provided within this GO.

NOTE: Under no circumstances shall an employee make a copy, record a copy (including the use of a personal device to record the video as it is played back), or permanently retain the contents of a video recording for personal use. Employees shall not post recordings to any external sources (e.g., social media sites), or provide recordings to personnel who are not members of the Department, except as otherwise provided within this GO.

e. Employee Access to Event Recordings. To refresh their memory of incidents, employees shall be allowed to review SCS recordings of their activity prior to the following:

(1) The preparation of written documentation requested or required by the Department.

(2) When SCS recordings are used as part of an administrative interrogation/interview, employees and/or their chosen representative shall be provided reasonable time, as well as the means, to view the recording(s), except for administrative interrogations/interviews conducted by the Department, as provided in paragraph 4.f.(3) of this GO.

(3) Providing formal (voluntary or compelled) statements as a victim or witness in an incident arising within the scope of the employee's official duties. For purposes of an officer-involved shooting or use of force case, officers will be considered victims or witnesses, and thus the Department may permit officers to review recordings of the incident prior to providing formal statements.

(4) Upon approval of a litigating attorney, preparing to testify in a criminal or civil proceeding, including preparing a response to civil discovery, arising from the employee's official duties.

f. Restricted Employee Access to Event Recordings. Access to SCS recordings will be restricted as follows:

(1) If a criminal investigation is being conducted, excluding those circumstances referenced in paragraph 4.e.(4)., it is within the sole discretion of the agency investigating the matter and the involved district attorney to determine if the employee will be allowed to view related video recordings.

(2) When an employee is charged with a crime, the employee may only review a related video recording if obtained from the district attorney prosecuting the matter in accordance with Sections 1054-1054.10 of the California Penal Code.

(3) When the CHP is conducting an administrative investigation in conjunction with an ongoing criminal investigation (excluding those circumstances referenced in paragraph 4.e.4.), employees may be allowed to review recordings of their alleged misconduct, prior to being charged with the appropriate Section 19572 GC offense, only after obtaining written permission from the Division Chief with oversight of the administrative investigation. If the Office of Internal Affairs is conducting the investigation, written permission shall be obtained from the Office of the Commissioner prior to release of the video recording(s).

5. CRIMINAL, CIVIL, AND ADMINISTRATIVE PROCEEDINGS. All requests for SCS recording files shall be accepted and processed in accordance with all laws and departmental policy.

a. Criminal Proceedings. Copying, viewing, and releasing of digital media maintained for evidence in criminal proceedings shall be coordinated through the district attorney's office.

(1) There will be no charge for evidence copied as a result of a criminal subpoena duces tecum or discovery order.

(2) The existence of video/audio recordings retained and kept as evidence for possible civil litigation must be disclosed to the prosecutor in a criminal proceeding. The discovery process shall be adhered to when releasing evidence. Copying, viewing, and releasing of such video evidence shall be coordinated through the Office of Legal Affairs (OLA).

b. Civil Proceedings. The copying, viewing, and releasing of recorded evidence for civil proceedings shall be coordinated through OLA. A fee may be required for copying digital media pursuant to a civil subpoena duces tecum or discovery order (refer to HPM 11.1, Administrative Procedures Manual).

c. Administrative Proceedings. When digital video/audio recorded evidence is used by the Department for the purpose of proving or disproving allegations of misconduct, only recordings relevant to the investigative scope shall be viewed and retained by investigators. Information relevant to the recordings viewed and seized as evidence by investigators shall be documented as part of the chronological summary of a criminal or administrative investigation. Upon request, employees subject to discipline, as defined by Section 19572 GC, shall be provided a copy of video and audio recordings utilized to support administrative sanctions when being served with a Notice of Adverse Action.

6. PUBLIC RECORDS ACT REQUESTS. Security Camera System video recordings may be withheld under the California Public Records Act (CPRA). A fact-specific inquiry is required. Therefore, personnel shall consult the Office of Risk Management, Public Records Act Unit (PRU), in connection with every CPRA request for video recordings. If a video is deemed to be releasable by PRU and redaction is required, a copy will be made, and all redactions shall be coordinated through PRU.

7. MAINTENANCE. It is vital to maintain the departmental SCS and ensure service continues and users are able to operate the system with minimal to no issues.

a. Repairs. If an issue arises and a camera is not recording or functioning, a user within the affected Area should first contact ITS and submit a ticket through Service Now. If ITS is unable to resolve an issue, employees should contact a Facilities Section representative. Upon notification, Facilities Section will contact the appropriate vendor for repairs and notify EOSS Section of the issue.

b. Cleaning. Industry standards dictate that cameras and their housing should be cleaned at least every three to four months. If cameras are exposed to more severe weather conditions, they should be cleaned more often to avoid any problems with capturing clear images. Area offices should work with the appropriate vendor(s) to establish a service contract for regular cleaning of the cameras and their housing.

8. MISUSE. The Area commander should be notified immediately if there are concerns over misuse of the SCS. Cameras are not to be viewed in a manner which would violate an individual's reasonable expectation of privacy as defined by law. Security cameras shall not be installed with the intent to conduct personnel investigations, such as those related but not limited to workplace attendance or work quality. However, the CHP may utilize security camera recordings captured during routine surveillance. This includes matters related to administrative investigations, investigations into violations of state or federal laws, or in a civil suit or other proceeding involving any person(s) whose activities are shown on the recording and relate to the proceeding.

9. TRAINING. When new users are added to the SCS, the EOSS Section shall provide training. This training can be either remote or in person and shall consist of the new user observing the instructor perform various routine functions within the SCS. Upon completion of training, users must demonstrate their familiarity with the SCS by performing essential functions, such as: selecting a camera to display a live image on screen, reviewing a previous time frame on a camera, and exporting camera footage. Users should not attempt to utilize the camera system prior to completing training with EOSS Section. The commander of any CHP facility with a standalone system will ensure their users receive appropriate training.

10. PRIVACY. Cameras are limited to uses that do not violate a reasonable expectation of privacy. Cameras may be installed in restricted access sites. Cameras shall not be located in bathrooms or locker rooms.

a. Placement of Cameras. Approved cameras can be both fixed and capable of having the view manipulated remotely. Where appropriate, cameras may be placed

inside and outside of buildings. The specific location of all cameras within a site shall be detailed in the CHP facility's Standard Operating Procedures (SOP) documentation. All CHP facility SOPs shall be updated by the commander or designee whenever changes to the locations of any camera are made.

b. Retention Period. The server shall store video recordings for 60 days. After 60 days, the server should overwrite data. All CHP facilities with standalone systems shall ensure video recordings are not retained longer than 60 days.

c. Camera Capabilities. The SCS can utilize cameras that record both video and audio data. Cameras purchased by the Department for use in CHP facilities shall only record video data. Audio data shall not be recorded. Any cameras installed that are capable of recording audio shall have that feature disabled. Cameras may have pan, tilt, and zoom functions which may be utilized by departmental employees during live viewings.

d. Remote Access. Remote access to a facility's SCS will only be granted with approval from the appropriate Division commander. In order to facilitate a request of this nature, an administrator for the SCS, working in conjunction with EOSS, will need to modify the user's account to grant permission to access other sites remotely.

e. Addition of Cameras. Any facilities that add cameras to the respective SCS shall update their Area SOP to reflect the addition of the cameras. Additional cameras that do not fall under the guidelines listed within this GO shall not be added to the system and do not fall under the purview of this GO.

OFFICE OF THE COMMISSIONER

OPI: 029