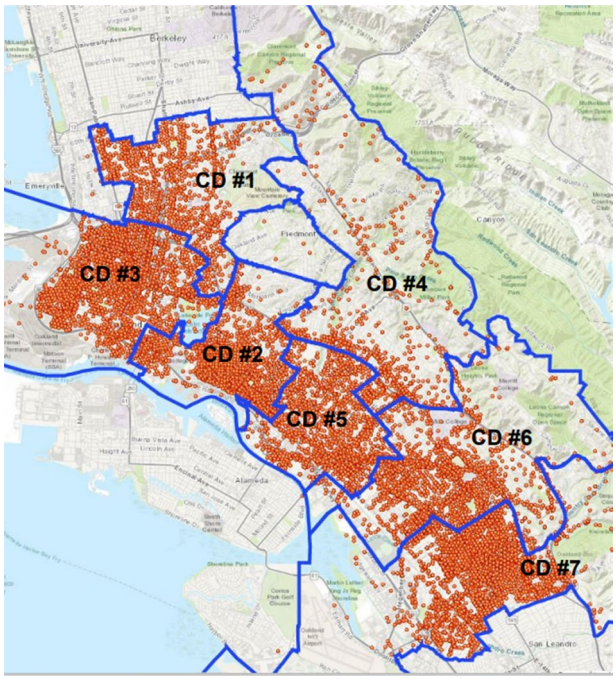
City of Oakland
Public Works Department Proposed Surveillance Technology Use Policy
for Illegal Dumping Surveillance Cameras

A. Purpose



FY21-22 Illegal Dumping Work Orders Completed by KOCB

Illegal dumping is a complex and multi-faceted problem that has been affecting the City of Oakland (City) for a number of years. City leaders have been working to develop a variety of strategies and programs to combat the rise of debris on city streets and public lands. This type of activity reduces the health and safety of Oakland's neighborhoods and disproportionally affects economically disadvantaged communities of color. The City's Illegal Dumping Surveillance Camera Program (Camera Program) is a critical component of these efforts. The goal of the Camera Program is to enforce against those who are illegally dumping debris throughout the city. The surveillance cameras offer the City a viable tool to enhance the investigative work performed by Oakland Public Works' (OPW's) Environmental Enforcement Unit (EEU) that is comprised of eight (8) Environmental Enforcement Officers (EEOs)*, a Clean Community Supervisor, and an Administrative Analyst. The EEOs are primarily tasked with enforcing illegal dumping using various tactics to hold illegal dumpers accountable for their actions, including forensic investigations involving thorough inspections of illegally dumped debris, and as of March 2022, monitoring video footage captured by surveillance cameras installed at illegal dumping hotspots throughout the city.

This is an updated Use Policy for the operation of the ***Portable Observation Device*** or POD – a surveillance system by Security Lines, U.S. – and seeks to add two products to the surveillance system to increase the efficacy and success of the camera program. These products are the Satellite PODs and License Plate Reader (LPR) cameras.

The goal of installing PODs, Satellite PODs and LPR Cameras near chronic dumping hotspots is to capture video evidence that identifies dumpers that produces supporting information needed to build credible cases for citations and prosecution. The issuance of citations and the prosecution of chronic illegal dumpers using video evidence serve as a deterrent to would-be dumpers who must weigh the benefits of dumping against the higher risk of getting caught by the cameras. By raising awareness of the presence of the

* Of the Eight (8) budgeted Full-time EEO positions, three (3) positions are currently vacant and are anticipated to be filled over the next six to nine months.

cameras and the frequency with which dumpers are caught and cited, the cameras will increasingly serve as an ongoing visual deterrent to potential dumpers.

Satellite PODs allow EEOs to increase viewing angles and viewable range to a dumping site by linking wirelessly one or more PODs to the main POD. Satellite PODs' additional point/tilt/zoom (PTZ) cameras are particularly useful when surveilling locations with multiple ingress and egress points or large stretches of roadway.

LPR Camera is a video camera with infrared lighting and filters that specializes in enhancing a license plate's readability. Surveillance data from March 2022 through February 2023 revealed that, of the 492 illegal dumping incidents captured by the PODs, 55% or 271 incidents were cases where citations could not be issued because EEOs were unable to see or read the license plate information clearly. Most often, the difficulty with reading license plates was a result of poor camera angles or poor video imaging. Adding Satellite PODs and LPR cameras to the current POD surveillance system will maximize the EEOs' ability to identify dumpers and to issue more citations.

B. Authorized Use

The use of the POD surveillance system, Satellite POD, and LPR camera is authorized solely for surveilling illegal dumping activity in the City of Oakland.

Only staff with a need to know and a right to know will have access to recordings captured by the POD system. See sections **D. Data Access,** and **H. Third Party Data Sharing**, for a list of individuals who will be authorized to access and/or view surveillance data.

Camera Placement: PODs are installed based on a hotspot list to maintain unbiased, non-viewpoint-based deployments. The hotspot list used is a ranked list of the most frequently dumped sites in Oakland. It is derived from analyzing top dumping locations based on the number of constituents' service requests and on the volume of KOCB work orders as per OPW's work productivity software Cityworks. The hotspot list is refreshed every two to three months to provide EEOs the most current dumping locations for camera placement. Additionally, cameras may be deployed at the Public Works Director's direction or for illegal dumping sting operations.

Redeployment: A POD is moved to the next location on the hotspot list once an EEO confirms there has been no recorded dumping for 14 consecutive days. Cameras remain in location until bucket truck-certified staff are arranged to move the POD.

C. Data Collection

Data collection occurs inside a POD housing unit. Video captured from the cameras are recorded directly to the digital video recorder's (DVR's) two (2) TB SATA hard drive. DVRs do not possess artificial intelligence (AI) or analytics such as facial recognition.

Audit Log – The audit log tracks system ties each action to a user for events such as:

- User Log-ins/ Log-outs by IP address
- User Management (add, edit, delete users; settings imported/exported)

Audit Log data resides locally on each DVR and requires an explicit query to be accessed. OPW owns the Audit Log data. It is accessible by password protected staff only.

Enforcement Data – Enforcement data is information that an EEO captures when he/she issues a citation or takes other enforcement action. Enforcement data is entered into custom fields in OPW's Cityworks application and is accessible by a query from City staff with Cityworks access. EEU staff also retain a manual log separate from Cityworks that shows when they check POD footage, if any dumping was found, and a brief description of the dumper(s) and dumped materials. The document is only accessible by EEU staff through a secure shared folder.

D. Data Access

Only designated City of Oakland staff have access to POD video data and LPR camera license plate data. The vendor cannot access the City's video data through the POD software. However, the vendor is authorized to temporarily access the surveillance system to provide ongoing technical support. Only the following individuals are authorized to directly access and/or view surveillance camera information:

Oakland Public Works –

- OPW Director and OPW Bureau of Environment's Assistant Director will be given access to view video data.
- KOCB Operations Manager, who oversees the EEU, will be able to add/delete users and will be granted admin/super user access.
- OPW Bureau of Environment's Administrative Services Manager, who administers the Illegal Dumping Surveillance Camera Use Policy, will be able to add/delete users and be given admin/super user access.
- EEU staff – Clean Community Supervisor, EEU Administrative Analyst, EEU Administrative Assistant, and EEOs – who will be tasked with checking cameras for illegal dumping activities and remote monitoring the POD units, will be given access to view video, control PTZ cameras, as well as search and download video evidence. EEU staff will not have the ability to add/delete users.

E. Data Protection

Since its introduction to the market in 2009, the POD surveillance system has never knowingly been hacked. POD DVRs are Linux-based; downloaded video is encrypted;

and video recordings cannot be played using standard video players (e.g., Windows Media Player).

There are three different levels of security to safeguard the POD's video data.

1. Cellular router level: An authorized user's computer must be recognized by the cellular router ("Router") before s/he can gain access to the POD system. Personnel with "admin/super user" profiles can specify which computers' IP addresses the Router recognizes. A unique username/password is required to configure the Router.

2. Desktop software level: To interface with the POD system, proprietary POD software is installed on an authorized user's computer. A unique username/ password is required to access software. Different levels of POD access – view only, PTZ camera control, video search & download, and admin/super user access – may be assigned to different personnel by the admin/super user.

3. DVR level (for mobile phone application only): Each POD has its own DVR. To access a specific POD's recordings, a separate log-in is required to access each DVR. Like the desktop software, users may be added or removed and given different levels of access.

Video data encryption takes place as the POD cameras record to the DVR. Satellite POD's video data is stored on the Main POD's DVR. LPR camera's video data will record to the POD's DVR, similar to PTZ cameras on a POD. The LPR camera's license plate data are enhanced images of license plates. These images are stored locally on a SD card inside the LPR camera and must be extracted from the LPR camera using a web browser interface. They are separate from the DVR data storage.

Downloaded video images and license plate information in the form of screenshots are stored in the Cityworks app as supporting documentation for citations issued. Downloaded video clips are saved to a secure EEU shared folder.

F. Data Retention

There are 3 ways video data are retained.

1. DVR hard drive: The POD DVR records video to the hard drive housed inside the POD unit. The hard drive automatically overwrites the oldest recordings every 14 days. Routine video recordings not downloaded are overwritten automatically and permanently by the DVR, when new video is saved on top of the oldest recordings.

2. Video from the License Plate Reader (LPR) camera is recorded to the POD's DVR, similar to the POD's other PTZ cameras and follows the same 14-day overwrite schedule. The enhanced license plate images are stored in the SD card inside the LPR camera, separate from the DVR. A SD card can store license plates data for

an average of 7-10 days before overwriting occurs. The actual number of days of storage, however, will depend on the number of license plates the LPR camera captures at the subject location.

3. Downloaded videos and images: Video will only be downloaded when it contains adequate illegal evidence of dumping to warrant possible enforcement actions. An authorized user will download the video clips via the POD desktop software to a secure OPW folder. License Plate information captured by LPR cameras will be downloaded from the web browser interface as an image. The image will include a picture of some, if not all, of the subject vehicle and the license plate information.

The POD cameras are not monitored in real-time. Video footage on each POD is reviewed by EEU staff Monday through Friday up to two times a day between the hours of 7am and 4pm. Screenshot photos of dumper, dumper's vehicle, dumped material, and license plate information used in citation and appeal processes will be stored as attachments in EEO Work Orders in Cityworks. Downloaded video clips are saved to a secure EEU shared folder and will be purged per legal guidance once filed claims, pending litigation, and/or criminal investigations and prosecutions conclude.

G. Public Access

Except where prohibited or limited by law, the public may access the City's video data through public records requests. However, prior to the release of any information to a surveillance-related public records request, staff will consult with the City Attorney's Office for review and guidance.

H. Third Party Data Sharing

Data may only be shared with the following departments or non-city entities in compliance with this policy: 1) City Attorney staff handling illegal dumping investigations; 2) City Attorney staff responding to a lawful court order or public record request; 3) Administrative Hearing Officer adjudicating illegal dumping cases; 4) Oakland Police Department and/or Alameda County District Attorney for illegal dumping investigations; 5) Vendor, solely to perform its contractual obligations; 6) At the discretion of the OPW Director, video data and license plate information may be shared with the City Administrator's Office and City Councilmembers. However, prior to the release of any information to a surveillance-related data request, staff will consult with the City Attorney's Office for review and guidance.

In the event POD cameras capture general illegal activity that reasonably appears to constitute "violent forcible crimes" as defined by OPD's Departmental General Order J-04 – Pursuit Driving Appendix A, Paragraph H: "Violent Forcible Crime," Environmental Enforcement Unit (EEU) staff shall promptly download the relevant video footage, forward said recording to OPD for possible investigatory and enforcement action, and log the incident. This log shall be incorporated into the annual report required by O.M.C. [Oakland

Municipal Code] 9.64.040.

Within 72 hours of any Oakland Police Department (OPD) request for video recordings, OPW shall notify the Chief Privacy Officer and Privacy Advisory Commission (PAC) Chair of the request. OPD's request will describe the nature of the investigation for which the video data is being requested. This information will be reported to the PAC at its next regularly scheduled meeting.

I. Training

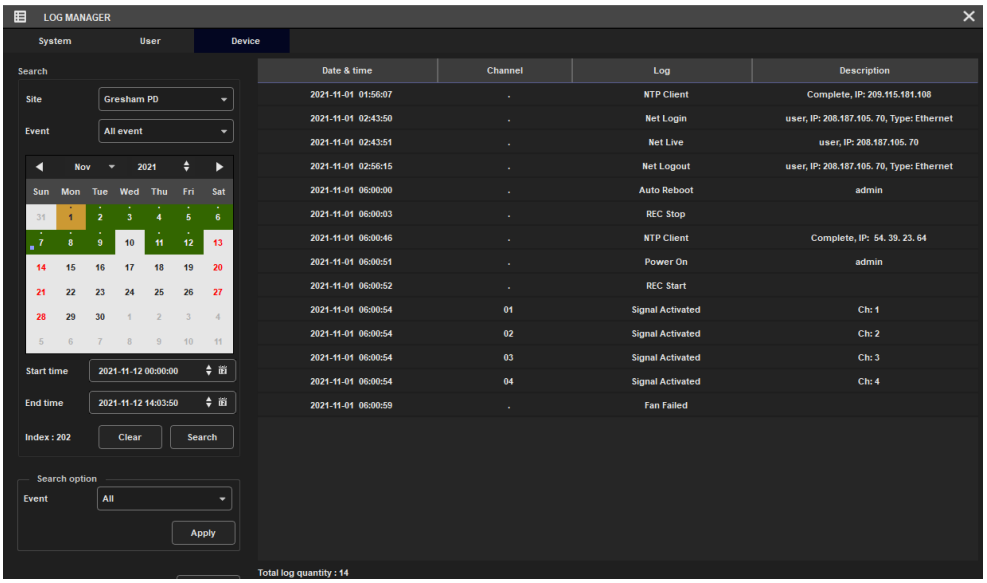
Training is available in video tutorials and written formats on vendor Security Lines U.S.'s website in a members-only area. One on one remote training is also available. The Administrative Services Manager in OPW's Bureau of Environment conducts training with authorized POD users as needed. Trainings include review of this Use Policy and reviewing operational procedures required to adhere to the Policy.

J. Auditing and Oversight

The Administrative Services Manager in OPW's Bureau of Environment shall conduct annual assessments to ensure authorized users comply with the Use Policy.

All POD user and device activity are logged. Designated admin/super users can access and view audit logs at the camera level.

Example of audit log.



The audit log tracks system ties each action to a user for events such as:

- User Log-ins/ Log-outs by IP address
- User Management (add, edit, delete users; settings imported/exported)

The audit log also tracks device specific events such as:

- Recordings stopped and started
- Reboots
- Power On
- Time syncs

K. Maintenance

Security Lines U.S. offers but does not require a maintenance contract. The POD's simple, rugged design requires minimal maintenance. Vendor and existing client testimonials suggest that maintenance, when required, constituted the occasional replacement of a hard drive or camera cover, which most client organizations service themselves.

However, as the City relocates the PODs more often than other agencies, staff is exploring a service contract with Security Lines, U.S. to provide routine equipment tune-ups, installation services, and system support to ensure reliable performance.