CITY OF OAKLAND

Privacy Advisory Commission

November 6, 2025; 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
Meeting Agenda

***Commission Members**: **District 1 Representative**: Vacant **District 2 Representative**: Don Wang, **District 3 Representative**:* Issac Cheng*, **District 4 Representative**: Lou Katz, **District 5 Representative**: Vacant, **District 6 Representative**: Gina Tomlinson, **District 7 Representative**: Sean Everhart, **Council At-Large Representative**: Henry Gage III, Vice Chair, **Mayoral Representative**: Jessica Leavitt, Chair*

Each person wishing to speak on items must fill out a speaker's card. Persons addressing the Privacy Advisory Commission shall state their names and the organization they are representing, if any. Members of the public can also raise their hand in Zoom if they have a question on an agenda item. The chair will determine the time allotted to speak on an agenda item.

1. Call to Order, determination of quorum

2. Open Forum/Public Comment on Non-Agenda matters

3. Action Items:
    a. Annual Reports
        1. CrimeTracer Forensic Logic 2024 (OPD)
        2. Illegal Dumping Surveillance Camera Annual Report (OPW)

    b. Use Policies
        1. Surveillance Technology Use Policy for Illegal Dumping Cameras (OPW)

Members of the public can view the meeting live on KTOP or on the City's website at https://www.oaklandca.gov/topics/ktop-tv-10.

Comment in advance. To send your comment directly to the Privacy Commission and staff BEFORE the meeting starts, please send your comment, along with your full name and agenda item number you are commenting on, to Felicia Verdin at fverdin@oaklandca.gov. Please note that eComment submissions close

one (1) hour before posted meeting time. All submitted public comment will be provided to the Privacy Commission prior to the meeting.

To observe and participate in the meeting via Zoom, go to: https://us02web.zoom.us/j/85817209915
Or One tap mobile: 1 669 444 9171

To participate in the meeting virtually, you must log on via Zoom. If you have a question, please raise your hand in Zoom during open forum and public comment.

For those attending in person, you can complete a speaker card and submit to staff.

CITY OF OAKLAND

MEMORANDUM

TO: PAC

FROM: Yun Zhou, Sergeant of Police
OPD, Criminal Investigation Division

SUBJECT: Forensic Logic CopLink / CrimeTracer System – 2024 Annual Report

DATE: May 12, 2025

Background

Oakland Municipal Code (OMC) 9.64.040: Surveillance Technology "Oversight following City Council approval" requires that for each approved surveillance technology item, City staff must present a written annual surveillance report for Privacy Advisory Commission (PAC). After review by the PAC, City staff shall submit the annual surveillance report to the City Council. The PAC shall recommend to the City Council that:

- The benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded.
- That use of the surveillance technology cease; or
- Propose modifications to the corresponding surveillance use policy that will resolve the concerns.

Oakland Police Department (OPD) Department General Order (DGO) I-24: Forensic Logic CopLink / LEAP, as well as OMC 9.64.040 together require that OPD provide an annual report to the Chief of Police, the PAC, and Public Safety Committee. The information provided below is compliant with these annual report requirements.

DGO I-24 explains that authorized members may use CopLink for the purpose of searching the system in the service of conducting criminal investigations, such as apprehending subjects, locating and returning stolen property, as well as in the protection of the law enforcement officers encountering the individuals described in the system. Authorized purposes also include other appropriate OPD organizational investigations (e.g., internal affairs, missing persons, and use of force investigations).

In 2023, CrimeTracer was introduced as the next iteration of CopLink. Forensic Logic also rebranded to SoundThinking. The product being used by OPD is now called SoundThinking CrimeTracer. OPD began migrating its user accounts in August of 2023 from CopLink to CrimeTracer. Functionally, it is the same product and consists of the same features and security. The only change made to the product is the name, logo and color scheme. Since the 2023 Annual Report, OPD has referred to the product as CrimeTracer.

Captain Nicholas Calonge, Criminal Investigation Division Commander, was the Program Coordinator for 2024.

A. **A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology**

CrimeTracer search technology is used regularly by both OPD sworn field / patrol personnel and command staff. Search parameters include the following criteria which are submitted to a search engine where data originating from law enforcement records, calls for service, field interviews, arrest/booking records and citations are stored:

- License plate numbers
- Persons of interest
- Locations
- Vehicle descriptions
- Incident numbers
- Offense descriptions/penal codes
- Geographic regions (e.g., Police Beats or Police Areas)

Data is stored in an FBI Criminal Justice Information Service (CJIS) compliant repository in the Microsoft Azure GovCloud.

In 2024, there were a total of 423 users accounts who conducted Forensic Logic searches, for a total of 204,750 separate queries. Table below breaks down this search data by month and by distinct user and total searches.

Table 1: OPD CrimeTracer Searches; by Distinct User and Search Totals – 2024

CrimeTracer

Search Type	***January***	***February***	***March***	***April***	***May***	***June***
Number of OPD distinct users in each month	*174*	*234*	*258*	*255*	*263*	*276*
Number of searches conducted	*15,068*	*15,838*	*17,104*	*17,386*	*20,604*	*18,278*

Search Type	***July***	***August***	***September***	***October***	***November***	***December***
Number of OPD distinct users in each month	*282*	*268*	*253*	*214*	*196*	*200*
Number of searches conducted	*19,756*	*19,443*	*18,521*	*16,646*	*12,563*	*13,543*

B. **Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):**

Data searched with the CrimeTracer system is entirely acquired from incident reports, citations, calls for service and field interviews that have already been recorded in originating Records Management Systems, Computer Aided Dispatch Systems, and Mobile Field Reporting Systems – from both OPD systems as well as from other law enforcement agency systems (other SoundThinking client agencies). The data is collected from OPD systems at least once every 24 hours; once the data is collected and resides in the SoundThinking

cloud repository, it is made available to agencies subscribing to the service who are permitted by their agency command staff to access CJIS information.

CrimeTracer does not keep statistics on who searched and viewed the data shared, but the system can be audited for a specific search.

Data sourced from the Oakland Police Department cannot be accessed by US DHS ICE nor US DHS CBP staff. Some federal agencies are using CrimeTracer with a limited licensing, meaning not every agents in the agency have access to CrimeTracer but the logins are assigned to various Federal Agents. These agencies are FBI, ATF, DEA, USPS, US Marshal and Secret Service.

Beyond federal access, CrimeTracer data is shared regionally with partner law enforcement agencies. Recipients include police departments, sheriff's offices, and state agencies across the following jurisdictions:

Los Angeles County, and agencies across Orange, San Bernardino, and Ventura counties

Santa Clara, Santa Cruz, Monterey, and San Benito counties, as well as agencies across San Francisco, San Mateo, Alameda, San Joaquin, Stanislaus, San Diego, and Fresno counties

State of Tennessee

State of Massachusetts

Maricopa, Pima, Pinal, and Yavapai counties in Arizona

Greater Kansas City region

Fulton and Cobb counties, Georgia

West and Central Oregon agencies

Spokane County, Washington

Reno, Sparks, and Washoe County, Nevada

El Paso and Houston, Texas

C. **Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to**

The CrimeTracer service is a web portal accessible by authorized OPD users on OPD computers with an appropriate user-id and password (criteria for both defined by FBI CJIS Security Addendum). OPD data sources that provide data accessible to the search tool include the following:

- Arrest records
- Field contacts

- Incident reports
- Service calls
- ShotSpotter Activations
- Stop Data reports
- Traffic Accident reports

D. **Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year**

Not applicable. The technology is a web portal that is accessible to computers on the OPD network.

E. **A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The PAC may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the PAC makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review.**

No community complaints or concerns were communicated to staff in 2024.

OPD is not able to provide the race of each person connected to each query. The technology is intended as a search engine of records (section C), not all queries would contain the race data of the person subject to the technology's use. OPD would have to individually evaluate tens of thousands of searches to provide the requested race data. Staff recommends the PAC makes the determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information.

F. **The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information**

No internal audit was conducted on CrimeTracer in 2024.

Staff was not made aware of any criminal or administrative investigation pertaining to the misuse of the technology in 2024.

G. **Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response**

There were no identifiable data breaches or known unauthorized access during 2024.

H. **Information, including case examples, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes:**

Homicide Case Examples

During the investigation of a homicide in the first quarter of 2024, the investigator searched CrimeTracer for prior incident reports involving the victim. One report detailed a recent argument involving the victim and another individual. A further search of field contact data showed the same individual had been contacted in the vicinity of the homicide scene days prior. This individual was later identified as the suspect and arrested.

During the investigation of a homicide in the third quarter of 2024, officers recovered a vehicle description from a witness. A CrimeTracer search of traffic accident reports found a recent collision involving a matching vehicle. The listed driver had prior arrests for firearm-related offenses. Further searches linked the driver to the scene, and the individual later identified as the homicide suspect.

Shooting Case Example

During the investigation of a shooting in the second quarter of 2024, the investigator reviewed prior ShotSpotter activations near the scene. A CrimeTracer search of field contacts within the activation radius showed an individual stopped minutes after a prior incident. That individual matched the description of the suspect provided by a witness. A review of prior arrests confirmed a history of gun-related charges. This information assisted in proving this individual to be the shooting suspect.

Burglary Case Examples

During the investigation of a residential burglary in the second quarter of 2024, officers identified a unique item stolen from the scene. A search in CrimeTracer showed a recent field contact where the same item was described in the narrative in the possession of a particular individual. Investigators followed up and later arrested the individual for the burglary.

Robbery Case Example

In the first quarter of 2024, patrol officers responded to a robbery where the suspect fled in a vehicle. The license plate was provided by a witness. A CrimeTracer search located a recent contact report involving the vehicle. One of the listed occupants had multiple prior arrests for robbery and was wearing clothing matching the description given by the victim. That individual was eventually arrested for the robbery.

I. **Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates**

There are no existing or newly opened public records requests relating to the technology.

J. **Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year**

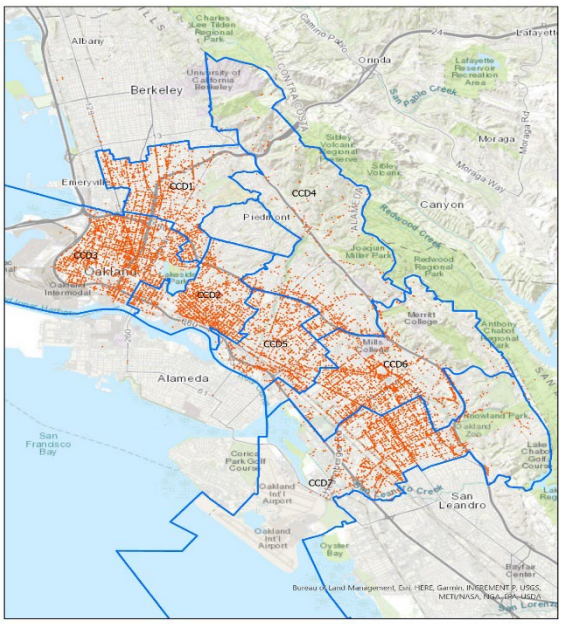
Description		Amount
Contract Start Date 7/1/2025	**Contract End Date** 6/30/2026	
197-0000-04 CrimeTracer	CrimeTracer Enterprise Subscription for Term 7/1/2025-6/30/2026	$227,500.00
197-0000-04 CrimeTracer	COPLINIK Connect	$10,000.00
197-0000-04 CrimeTracer	CompStat, per user subscription (60 users @ $1,000 each)	$0.00
197-0000-04 CrimeTracer	General Purpose and Maintenance Services	$25,000.00
	Total	**$262,500.00**

K. **Any requested modifications to the Surveillance Use Policy and a detailed basis for the request**

No requests for changes at this time.

City of Oakland
Public Works Department Surveillance Technology Use Policy for Illegal Dumping Surveillance Cameras
Revised October 29, 2025

A. Purpose



FY 24-25 Illegal Dumping Work Orders Completed by KOCB*

Illegal dumping is a complex and multi-faceted problem that has been impacting the City of Oakland (City) for several years. City leaders have been working to develop strategies and programs to combat the rise of debris on city streets and public lands. Illegal dumping 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 document and enforce against those who illegally dump 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) Recycling and Environmental Enforcement Program known as the Environmental Enforcement Unit (EEU) that is comprised of seven(7) budgeted 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 Use Policy covers the operation of the ***Portable Observation Device*** (POD) which include Satellite PODs, and PODs with License Plate Reader (LPR) technology. The surveillance system is procured and installed by Security Lines US (SLUS).

The goal of installing PODs, Satellite PODs and LPR Cameras near chronic dumping hotspots is to capture video evidence that identifies dumpers producing 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.

** Of the seven (7) budgeted full-time EEO positions, three (3) positions are currently vacant, 2 of which were frozen due to budgetary constraints. The current FY 25-26 approved budget now allows these positions to be filled.*

By raising awareness of the presence of the 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. The technology was deployed to increase visibility and clarity of license plate information captured by cameras.

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 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 may be moved to the next location on the hotspot list once 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 network video recorder's (NVR's) four (4) TB SATA hard drive.

The LPR POD model is not capable of analytics such as facial recognition and private property is manually blurred.

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

D. Data Access

Only designated City of Oakland staff have access to POD video data and LPR camera license plate data. Under a 3-year technical support contract, SLUS technicians have access to the surveillance system and video data on an as-needed basis. During the fiscal year 2024-2025 reporting period, 15 new cameras were installed putting a total of 30 cameras in service without additional staff to monitor them daily. Consistent and reliable camera monitoring was needed. To solve the problem, SLUS technicians began providing the added service of downloading video data as a spreadsheet providing EEU staff data capturing illegal dumping activity each day from all cameras. This monitoring system increases the speed, efficiency and number of citations issued each day allowing EEU staff to focus on the investigation necessary at times to ensure that the dumper as well as the waste generator are held accountable.

The following individuals are authorized to 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.
- Environmental Services Manager and Recycling Program Manager, who oversee the REEP, will be able to add/delete users in accordance with the data access needs outlined in this section, and will be granted admin/super user access.
- REEP staff – Clean Community Supervisor, REEP Administrative Analyst, REEP Administrative Assistant, REEP Recycling Program Specialist I (new), and EEOs – who are tasked with checking cameras for illegal dumping activities and remote monitoring the POD/LPR POD units – will be given access to view video, control PTZ cameras, as well as search and download video evidence. REEP staff will not have the ability to add/delete users.
- Security Lines US. – Technical staff for as-needed technical support and will pull data documenting illegal dumping daily and provide only the license plate and location data to REEP staff. REEP staff currently have access to view and download video evidence.

E. Data Protection

POD NVRs are Linux-based. Downloaded video is encrypted, and video recordings can 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. NVR level (for mobile phone and web browser applications): Each POD has its own NVR. To access a specific POD's recordings, a separate log-in is required to access each NVR. 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 NVR. Satellite POD's video data is stored on the Main POD's NVR. LPR camera's video data will record to the POD's NVR, like PTZ cameras on a POD. The LPR camera's license plate data are enhanced images of license plates. These images are also stored locally on the POD's hard drive.

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 three ways video data are retained.

1. NVR hard drive: The POD NVR 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 NVR, 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 NVR, like the POD's other PTZ cameras and follows the same 14-day overwrite schedule. The enhanced license plate images are stored in the POD's NVR.

   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 NVR. The image will include a picture of some, if not all, of the subject vehicle and the license plate information.

POD cameras are not monitored in real-time. Video footage from each POD is captured by SLUS Monday through Friday up to two times a day between the hours of 7am and 4pm. License plate and location information is downloaded in an Excel spreadsheet and sent to EEU staff for further investigation and citation issuance. Screenshot photos, retrieved by EEU staff, 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 the 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

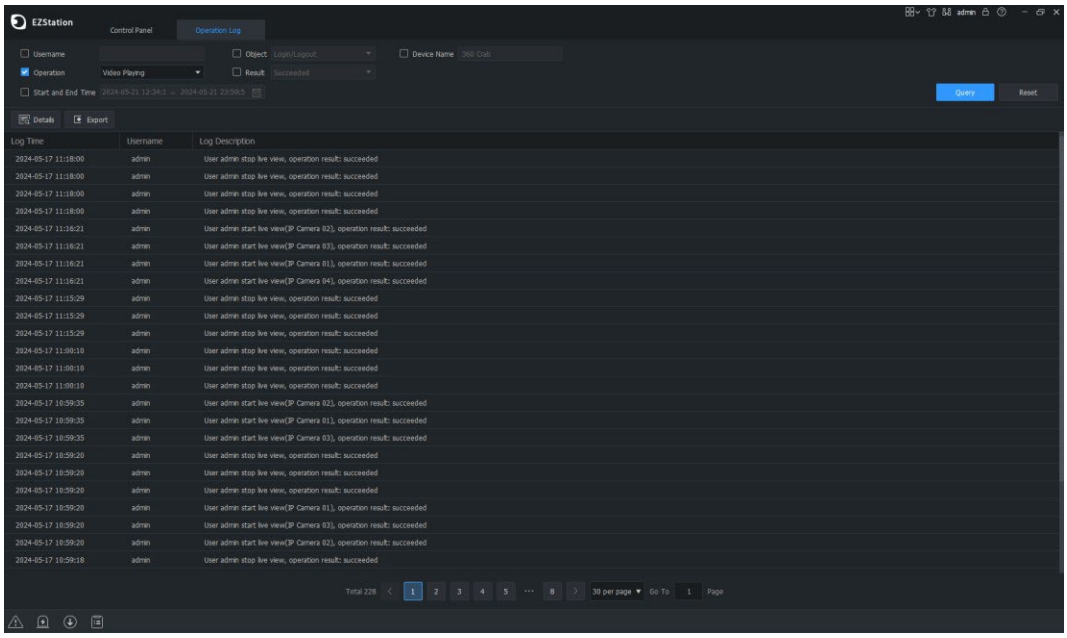
Training is available in video tutorials and written formats on vendor Security Lines US's website in a members-only area. One-on-one remote training is also available. OPW staff will conduct periodic training with authorized POD users as needed. Trainings include review of this Camera Use Policy and reviewing operational procedures required to adhere to the Policy.

J. Auditing and Oversight

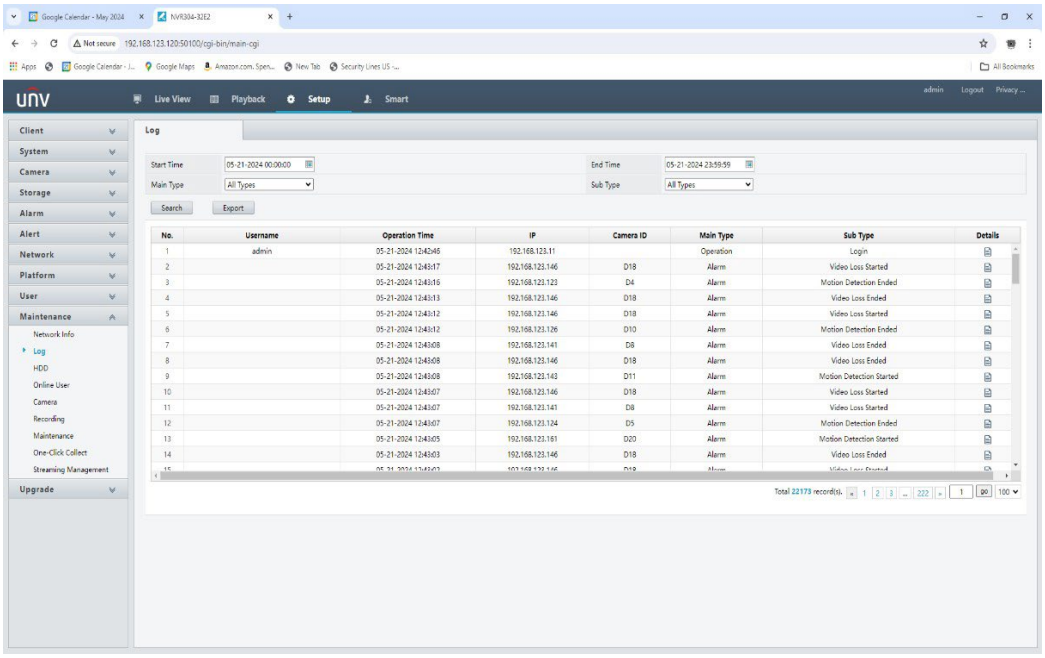
The Environmental Services Manager or assigned staff shall conduct annual assessments to ensure authorized users comply with the Camera Use Policy.

There are two logs with the POD/LPR POD upgrade. All user and device activity are logged in the EZStation software. Designated admin/super users can access and view audit logs at the camera level.

Example of EZStation audit log.



There is a second log inside each NVR which logs actions from the specific POD with which the NVR is paired.



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

- User Logins/Logouts 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

The POD's/ LPR POD's simple, rugged design requires minimal maintenance. However, as the City relocates its PODs more often than other agencies, EEU staff are routinely experiencing logistical challenges such as insufficient power source and poor cellular signals that impact camera deployments. To address these challenges, OPW has a three (3) year technical service contract with Security Lines US to provide routine equipment tune-ups, installation services, and system support to ensure reliable performance.

OPW Illegal Dumping
3rd Annual Surveillance Camera Report

CITY OF OAKLAND
PUBLIC WORKS

PROGRAM IMPLEMENTATION

Report for April 2024 – March 2025

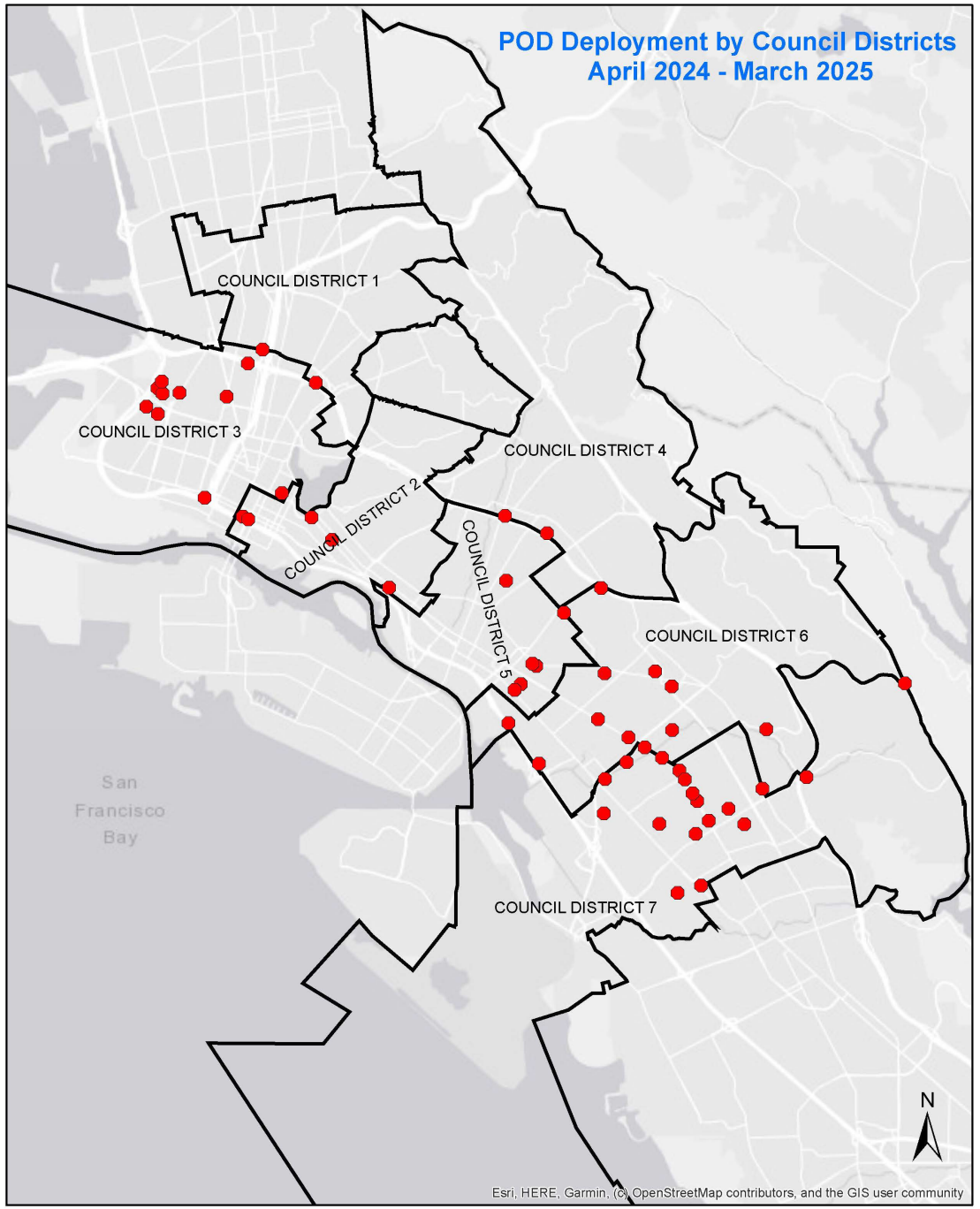
- System Use
- Deployment
- Community Complaints
- Data Breaches
- Efficacy
- Public Records Requests
- Use Policy Amendment

SYSTEM USE & DEPLOYMENT

- 36 Cameras:
  - 15 Additional Cameras
  - 6 Reserve Cameras
- Deployment Strategy:
  - Illegal dumping reports to OAK 311 + field intel → Cityworks/data-driven chronic hotspots
  - OPW Directive

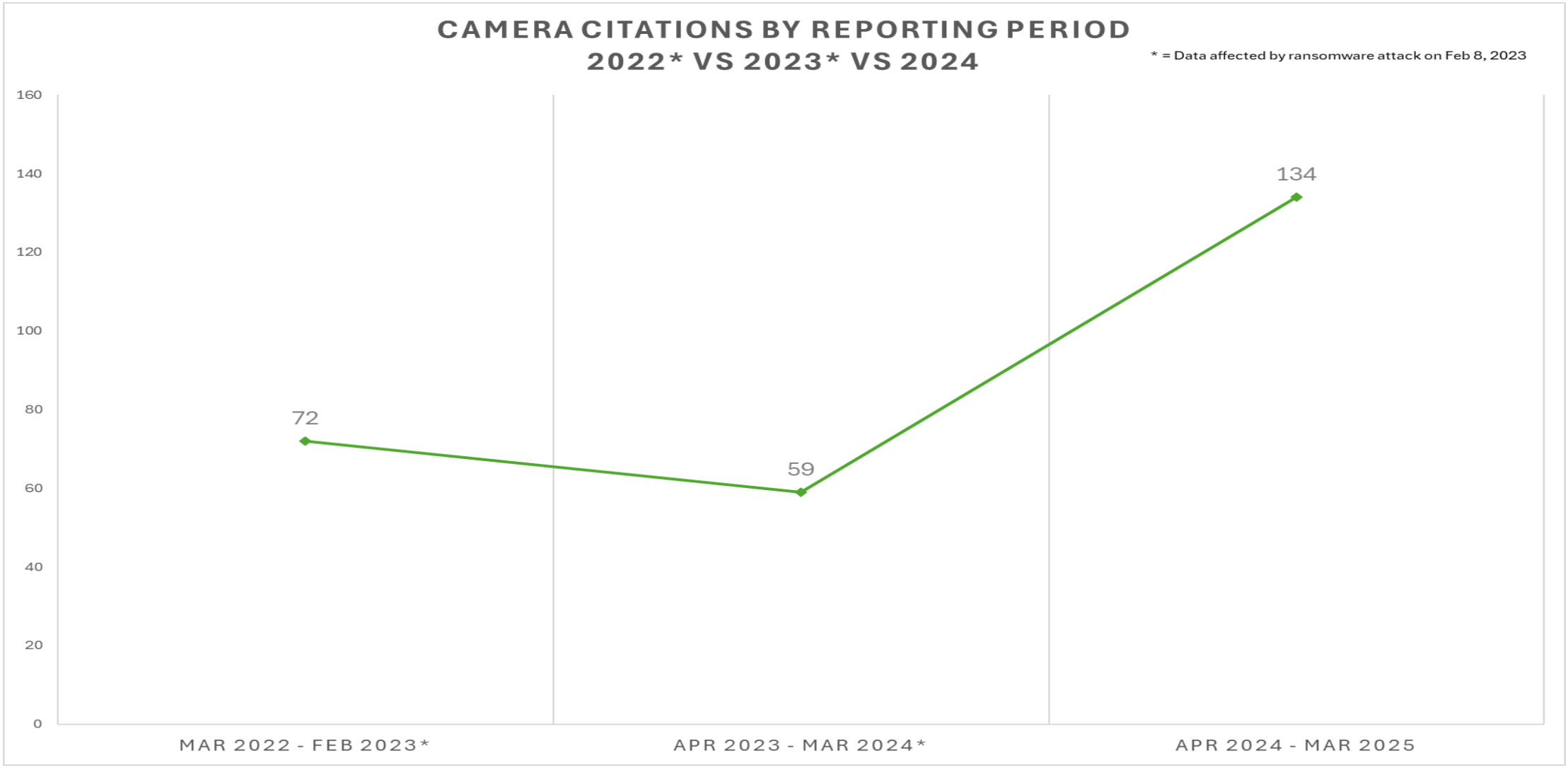
POD DEPLOYMENT

- 52 Total Deployments:
  - Data-driven deployments @ identified hotspots
  - 1 Director requested deployments

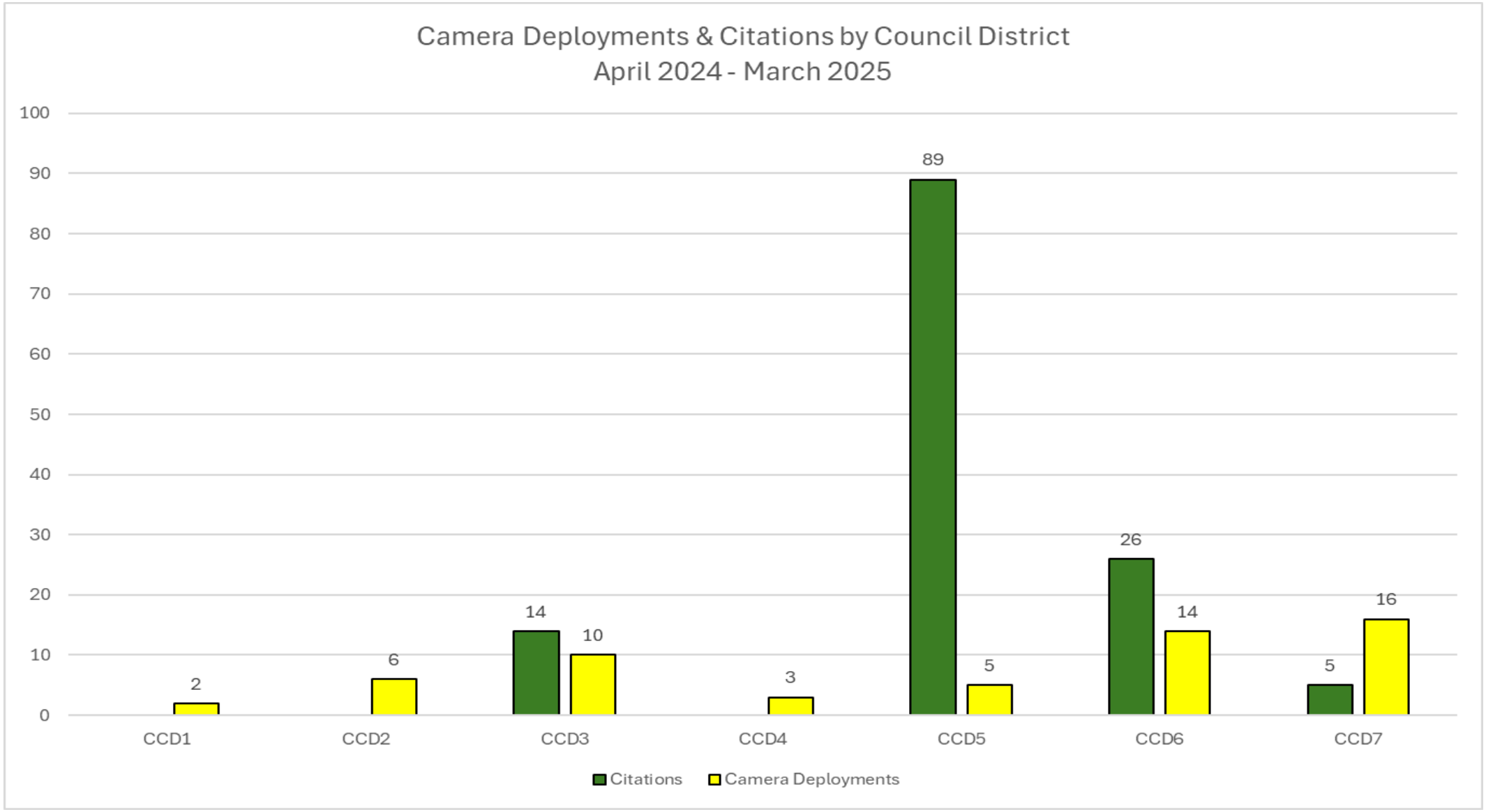


Created by GIS Team: 9/16/2025

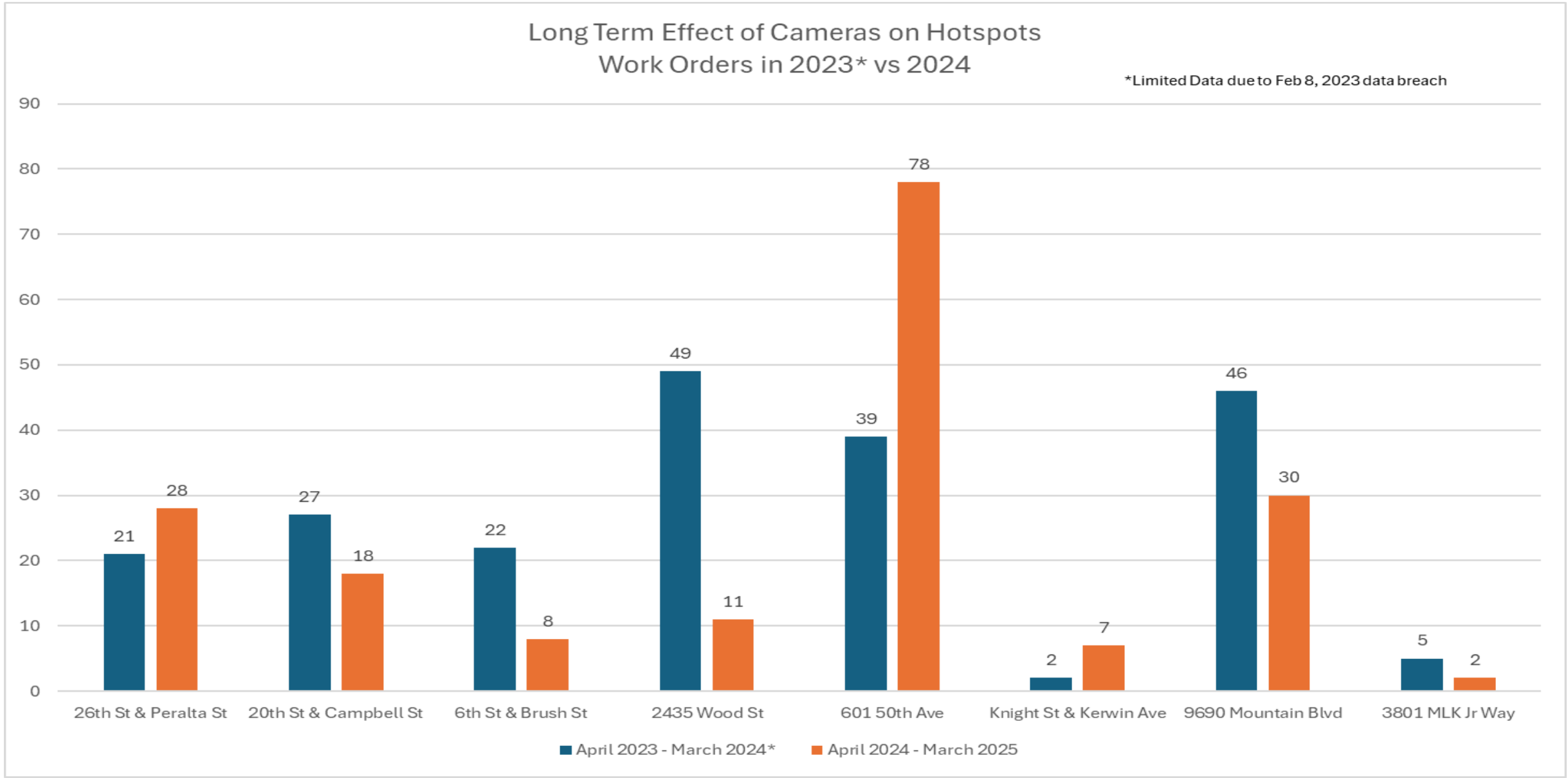
SURVEILLANCE CAMERA EFFICACY



SURVEILLANCE CAMERA EFFICACY



SURVEILLANCE CAMERA EFFICACY



STOLEN CAMERA/DATA BREACH/PRIVACY COMPLAINTS

- *No cameras were stolen*
- *No Data Breaches*
- *No Privacy Complaints*
- *1 Public Records Request*
  - *No video footage requested*

USE POLICY - PROPOSED AMENDMENTS

Modify provision in:

- *Section D. Data Access* – expanded permission for user currently authorized to access and/or view surveillance camera information
- Additional permission to:
  - Review camera video
  - Download data
  - Report to City

LPR Camera

QUESTIONS

Wanda Redic

Oakland Public Works – Recycling & Environmental Enforcement

CITY OF OAKLAND
PUBLIC WORKS