Annual Surveillance Report

San Diego Police Department

2025

Introduction

Executive Summary

Introduction

Surveillance technologies are an important part of modern policing, helping officers respond to emergencies, investigate crimes, and protect the public. Required under the City of San Diego's Transparent and Responsible Use of Surveillance Technology (TRUST) Ordinance, this 2025 Annual Surveillance Report describes how the San Diego Police Department uses these tools responsibly and with safeguards designed to protect privacy and civil rights.

As defined by the TRUST Ordinance, a surveillance technology is "any software, electronic device, or similar that observes, collects, retains, analyzes, processes, or shares information such as audio, electronic, visual, location, thermal, olfactory, biometric, or similar information capable of being associated with any individual or group. It also includes the products of these surveillance technologies."

These technologies play a critical role in the Department's daily operations by supporting responses to public safety incidents, helping de-escalate critical situations, and assisting in the investigation and resolution of crimes. They enhance situational awareness, support investigations, and provide actionable evidence after crimes have occurred. Their use also allows the Department to operate more effectively and efficiently, particularly in an environment of limited staffing and increasing service demands.

At the same time, the value of these tools requires equally strong policies and safeguards to govern their use. This report not only explains how surveillance technologies are used, but also outlines the policies, controls, and accountability measures in place to ensure they are used responsibly and legally.

This report reflects the TRUST Ordinance's oversight framework, which requires surveillance technologies to undergo a rigorous and transparent review process before they're able to be used. That process includes public disclosure, collaboration with the Privacy Advisory Board, and City Council approval. Through structured review and community engagement, potential risks are identified, safeguards are strengthened, and policies evolve to reflect best practices and community expectations.

Over the past year, this process resulted in meaningful improvements to Department use policies, auditing practices, reporting standards, and public transparency. These changes strengthened accountability and reinforced compliance with applicable state and local laws, including data-sharing restrictions consistent with the California Values Act and SB 34.

This work underscores the TRUST Ordinance's role as a framework for ongoing evaluation rather than a one-time review. By engaging in structured oversight, public input, and iterative policy updates, the Department continues to strengthen governance while preserving the operational value of surveillance technologies as essential tools for public safety.

All surveillance technologies included in this report have been authorized under the TRUST Ordinance. This ordinance establishes the definitions, reporting requirements, oversight mechanisms, and accountability measures that guide the Department's use of these technologies, including the requirement to publish this Annual Surveillance Report.

Table of Contents

San Diego Police Department
Air Support Unit (ASU)

SDPD

ONE TEAM. ONE MISSION.

San Diego Police Department

Avalex DVR & and FLIR 380HDc

Department/Division: Police – Special Operations – Air Support Unit

Related Policy/Procedure:

- DP 1.01- Department Directives
- DP 1.45- Use of City/Department Computer Systems
- DP 3.26- Media Evidence Recovery and Impounding/Preserving Procedures

---

DESCRIPTION

The Avalex DVR is a helicopter-mounted technology providing the Department's Air Support Unit (ASU) the ability to record and playback audio (which includes police radio traffic, aircraft tower traffic, and internal communication(s) between crewmembers), and imagery produced from the helicopter-mounted forward-looking infrared (FLIR) sensor during police-related incidents. The FLIR 380HDc sensor is an externally mounted camera system that produces infrared and color video imagery. The two technologies function together and are used on every ASU patrol flight. 441 impounds of videos were made between January 1, 2025, and December 31, 2025. Of those videos, approximately 226 videos were uploaded to Evidence.com for release to investigators or prosecutorial agencies.

ASU flew 2,637 hours in the 12 months between January 1, 2025, and December 31, 2025, covering the City of San Diego, along with San Diego County, in our role as a regional asset. The FLIR sensor is powered on at aircraft start-up and deployed on every flight. The Avalex is manually set to record by the Tactical Flight Officer when the air crew is on an incident where captured imagery may be used in a criminal investigation. Neither of these technologies have the ability to save, track, analyze, or capture data on the location of use, duration of use, or the configuration of use for these items.

SHARING OF DATA

Data recorded to the Avalex DVR via the FLIR 380HDc sensor includes incidents that are of possible evidentiary value in criminal cases. ASU has only shared recordings with authorized law enforcement agencies upon supervisor approved written requests. Due to the evidentiary nature of the videos, the approved video requests are uploaded to Evidence.com for the requestor to access. No impermissible 3rd party sharing has occurred. ASU only grants access to the data saved on the Avalex DVR system in accordance with California State Law, San Diego Police Department Policy or Procedure, or the Use Policy.

Of the 441 impounds of videos, 88 ASU videos were shared with outside law enforcement agencies during 2025, between January 1, 2025, and December 31, 2025. The videos were uploaded to Evidence.com and a secured link is sent to the law enforcement requestor as evidence in criminal investigations.

Agency	Number of cases
Carlsbad Police Department	1
Coronado Police Department	1

Agency (continued)	Number of cases
Chula Vista Police Department	7
California Highway Patrol (CHP)	32
Department of Justice (DOJ)	1
El Cajon Police Department	1
Escondido Police Department	1
La Mesa Police Department	3
National City Police Department	5
San Diego County District Attorney's Office	23
San Diego County Sheriff's Office	3
San Diego State University (SDSU) Police Department	1

LOCATION

The Avalex DVR is a helicopter-mounted technology used to provide the ASU the ability to record and playback audio (which includes police radio traffic, aircraft tower traffic, and internal communication(s) between crewmembers), and imagery produced from the helicopter-mounted forward-looking infrared (FLIR) sensor during police-related incidents. The FLIR 380HDc sensor is an externally mounted camera system that produces infrared and color video imagery.

UPDATES, UPGRADES, AND CONFIGURATION CHANGES

There have been no updates, upgrades, or configuration changes that expanded or reduced the surveillance technology capabilities.

DEPLOYMENT LOCATION

The Avalex DVR and FLIR 380HDc are mounted on department aircraft and are operational during flight and are utilized throughout San Diego County as a regional asset. The primary mission is to provide air support for the San Diego Police Department, which includes all SDPD service areas and Council Districts.

COMMUNITY COMPLAINTS OR CONCERNS

The Department is committed to protecting civil rights and liberties of our citizens as presented to the City Council prior to approval of this technology. The Department has not received any complaints or concerns about this surveillance technology or received any reports of disproportionate impacts. The Use Policy continues to protect civil rights and civil liberties.

AUDITS OR INVESTIGATIONS

In response to the Privacy Advisory Board's (PAB) Memorandum addressed to San Diego City Council President LaCava and Members of the San Diego City Council on April 17, 2025, which provided a request for more rigorous auditing processes, the SDPD's Research, Analysis, and Planning Division published Department Order (OR) 25-13 on April 25, 2025. This order requires the managing unit (the managing unit is the person(s) recognized as the subject matter expert (SME) for the Transparent and Responsible Use of Surveillance Technology ordinance reporting or who controls the equipment) to prepare for the required Annual Report each year. The OR requires that the SMEs conduct quarterly audits of the equipment they are in charge of, including compiling and tracking information and data listed in SDMC 210.0102(a). On July 15, 2025, an additional Department Order, DO 25-23, was published. This DO requires Department members using any technology or database to enter a reference code/ID or justification for use of the technology or database with either a relevant full eight-digit case number, a full 11-digit event number, or other unique identification code. It requires that users no longer use nonspecific phrases or references and enhances the ability to audit the system.

In accordance with OR 25-13, and as an addition to the required quarterly audits by the managing unit, an independent audit was conducted by the Research, Analysis, and Planning Division (RAP)– Inspection and Control Unit. The audits were in addition to the quarterly audits required by the managing unit in OR 25-13. These audits targeted confirmation of the proper use of the technology, as stated in the Use Policy.

This technology is monitored by the Air Support supervisors and is regularly monitored to verify the proper use of the technology. Any video from this technology is uploaded to Evidence.com, when collected as evidence and catalogued. All other videos are downloaded onto a hard drive and kept in a secure location in the Air Support Unit. No unauthorized uses of the technology were located during the audit conducted by RAP.

Any training issues or unintended input errors with this technology were identified and corrected. Continued errors or training issues will result in the user being suspended from the technology until they can be retrained on the technology.

Any substantial non-compliance or intentional misuse will be forwarded to the command or the Internal Affairs Unit for investigation and the subject may have their access permanently removed from the technology.

There was no unauthorized access of this technology and/or no located or reported violations of the Surveillance Use Policy or SDPD Policy or Procedure regarding this technology.

DATA BREACH OR UNAUTHORIZED ACCESS

The City of San Diego's Department of Information Technology and SDPD Information Technology Unit has identified no data breaches or unauthorized access to the data collected by the surveillance technology.

DATA BREACH DETECTION

The City's Department of Information Technology oversees the IT governance process and works with SDPD's Department of IT regarding project execution and risk assessment as well as selecting and approving technology solutions. Cyber security and technology risks are also

assessed by the Department of IT. For additional details related to IT governance processes, refer to the information at the following link:

https://www.sandiego.gov/sites/default/files/fy23-fy27-it-strategic-plan-sd.pdf

INFORMATION AND STATISTICS

There are no direct relational crime statistics associated with or produced by the use of this technology.

Should the public want to access crime statistics for the City of San Diego, they can visit the City's *Crime Statistics & Crime Mapping* webpage: Crime Statistics & Crime Mapping | City of San Diego Official Website. The City's neighborhood crime summary dashboard is available at: San Diego Neighborhood Crime Dashboard (arcgis.com). A tab on this dashboard, Crime Data Explorer, allows the user to query crimes specific to a City neighborhood.

Additionally, crime data is also available on the City's Open Data Portal: Datasets - City of San Diego Open Data Portal. This crime data can be downloaded into usable files; also available on this site are dictionaries to help navigate the different data sets.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

There were ten (10) California Public Records Act requests referencing these technologies in 2025. The information produced in response to these requests can be viewed on the City of San Diego's CPRA request portal: https://sandiego.nextrequest.com/

Request Number	Requested Date	Closed Date
25-553	1/23/2025	2/22/2025
25-45	1/03/2025	1/30/2025
25-8664	11/03/2025	11/28/2025
25-6853	9/03/2025	9/20/2025
25-6778	9/01/2025	9/13/2025
25-4473	6/10/2025	6/21/2025
25-2280	3/24/2025	3/28/2025
25-705	1/28/2025	Open
25-7858	10/07/2025	11/25/2025
25-3165	04/23/2025	05/13/2025

ANNUAL COST

All five FLIR 380HDc sensors were purchased with federal grant money. All five are maintained with either a Service Maintenance Agreement (SMA) or warranty through the manufacturer, Teledyne FLIR, and paid by the department's General Fund. The annual cost for the FLIR 380 HDc sensors is approximately $155,000 for all five units.

The Avalex DVR has no yearly cost, except when service is needed. The Department currently has six (6) DVRs.

REQUESTED MODIFICATIONS TO THE USE POLICY

There are no requested modifications to these technologies' Use Policies.

Department/Division: Police – Special Operations – Unmanned Aircraft System Unit

Related Policy/Procedure:

- DP 1.01- Department Directives
- DP 1.25- Inspections and Audits Protocol
- DP 1.45- Use of City/Department Computer Systems
- DP 1.49- Axon Body Worn Cameras
- DP 1.57- Military Equipment
- DP 3.02- Impound, Release, and Disposal of Property, Evidence, and Articles Missing Identification Marks
- DP 3.26- Media Evidence Recovery and Impounding/Preserving Procedures
- DP 6.04- Case Report Form
- DP 6.06- Crime Scene Protection and Preliminary Investigation Reporting
- DP 8.23- Use of Small Unmanned Aircraft System
- DP 9.03- Obedience to Laws Policy
- DP 9.28- Department Reporting Policy

DESCRIPTION

An Unmanned Aircraft Systems (UAS) is defined by Public Law 112-95, Section 331(8) as an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft. The Federal Aviation Administration classifies all UAS that weigh under 55 lbs. as "Small UAS." All of the UAS used by the San Diego Police Department fall under this FAA classification of "Small UAS." Most UAS have a digital camera attached or designed as part of the aircraft.

A UAS is, in essence, a manually controlled video/photography camera that is attached to a small remote-controlled aircraft. The majority of the data collected by UAS is similar to a handheld "point-and-shoot" camera or a Body Worn Camera.

For the 2025 calendar year, the San Diego Police Department used the following UAS makes and models during operations:

- DJI Matrice 30T
- DJI Mavic 2 Enterprise Advanced
- DJI Mavic 3 Enterprise
- Hoverfly Sentry HL
- DJI Avata v2
- Teledyne FLIR Black Hornet PRS

All of SDPD's UAS have the below common features:

1. They all weigh less than 25 lbs in weight, including all batteries and payload.

2. They all have a quad-copter design and use 4 electrically motorized propellors to provide lift.

3. They are all equipped with digital cameras capable of taking photographs and videos in the visual spectrum, and the majority of them have some zoom capability.

4. All models are not exclusively sold to military and police agencies, and the majority of the models can be acquired by the general public "off the shelf."

Some of the UAS models that SDPD uses have additional features and capabilities.

The following UAS have an additional camera sensor that can take photographs and video in the Forward Looking Infrared (FLIR) spectrum, commonly known as "thermal imagery":

- DJI Matrice 30T
- DJI Mavic 2 Enterprise Advanced
- DJI Mavic 3 Enterprise
- Hoverfly Sentry HL
- Teledyne FLIR Black Hornet PRS

The following UAS have an additional camera feature that can take photographs and video in the Infrared spectrum commonly known as "IR," "Night Vision," or "Low-Light":

- DJI Matrice 30T
- Hoverfly Sentry HL

In 2025, UAS Technology was deployed to 120 incidents. UAS camera technology was utilized for 119 of these 120 incidents. Of the 120 incidents that camera technology was used, at 85 of the incidents evidence was collected in either video or photographic form, while at the other 34 incidents the UAS camera technology was used for observation only and did not record any evidence.

UAS technology was physically flown for 114 of these 120 incidents, while UAS camera systems were used in a non-flight capacity for 5 of these incidents, and for the remaining 1 incident the UAS technology was deployed to an incident but not utilized in any capacity.

Of the 120 incidents, four of them were requests to support outside law enforcement agencies or city departments other than the San Diego Police Department. Of the 120 incidents, 14 of them were conducted in locations outside of the city of San Diego.

The four requests to support outside law enforcement agencies or city departments other than the San Diego Police Department were:

- January 4, 2025 – The Riverside Police Department (RPD) conducted a warrant operation in San Diego and requested SDPD UAS Unit assistance.

- April 3, 2025 – The La Mesa Police Department (LMPD) SWAT Unit requested the SDPD UAS Unit to fly for overwatch during their warrant service operation.

- May 5, 2025 – The Federal Aviation Administration (FAA) and the National Traffic Safety Board (NTSB) responded to a plane crash in the Murphy Canyon area and requested UAS Unit to assist with overhead photographs of the crash scene to support their aviation investigation. These photos were shared with the FAA and NTSB investigator.

- December 10, 2025 – The San Diego County Sheriff's Office (SDSO) had an officer-involved shooting and the SDPD UAS Unit was asked to assist with crime scene evidence collection by the SDPD Homicide Unit.

The Dejero Downlink Transmission System (DTS) is a live video transmission system, based on bonded cellular network technology. The Dejero DTS consists of three pieces of hardware: a transmitter, a receiver server, and a video management server. The Dejero DTS does not contain any cameras or microphones; the only video transmitted is via the UAS during authorized SDPD UAS Operations or Training. The Dejero DTS was used on 71 of the 120 incidents. The Dejero DTS did not collect or retain any evidence at any of these incidents and was used for live video transmission only from the UAS.

UAS Technology and the Dejero DTS were utilized for the following mission types and objectives in 2025:

- Support SWAT Unit during incidents involving a barricaded suspect believed to be armed.
- Support SWAT during a high-risk warrant services.
- Searches for at-risk missing adult.
- Searches for at-risk missing juvenile.
- Aerial Overwatch at mass gathering special events to detect terrorism and criminal activity.
- Searches for fleeing felony suspect believed to be armed.
- Capture video and photographic evidence of major crime scenes.
- Support FAA and NTSB with evidence collection photographs of a plane crash incident.
- Observe civil demonstrations to provide situational updates to incident commanders.
- Remotely inspect suspicious packages believed to be improvised explosive devices.
- Search for a suspect's discarded firearm to find evidence and support public safety.

SHARING OF DATA

Data collection, Data Access, Data Protection, Data Retention, Public Access, and Third Party Data Sharing for all UAS platforms is listed in the Surveillance Use Policies.

During Calendar year 2025, all video and photographic digital media evidence that was collected in response to a Law Enforcement Operation was impounded as evidence in accordance with Department procedures and labeled with regard to the individual associated investigation and case number. After the digital media evidence has been impounded, the sharing of the individual data files is at the discretion of the investigator assigned to each individual case in accordance with department procedures.

For the operation with the FAA/NTSB on May 5, 2025 (Listed in the Description section above), photography was taken and retained but it was not captured as law enforcement-related evidence to a crime. The digital media that was taken was in support of Federal Aviation investigation efforts.

The operation was not for immigration purposes and was compliant with the California Values Act, California FACE Act, and SB 34.

LOCATION

For the majority of the SDPD UAS aircraft models, UAS related digital media evidence is originally collected onto a physical SD card located on the UAS. At the conclusion of the operation, UAS staff physically uploads the digital media evidence onto a thumb drive and physically impounds it in the property room, or digitally uploads the evidence onto the evidence.com system. After the transfer is complete the UAS SD card is wiped.

For a few UAS systems, primarily the Hoverfly Tethered UAS, video and photographic digital media evidence is not stored onto the UAS at any time. Digital media evidence is collected onto an SD Card that is located an external video recording device that is connected to the UAS ground control station at the time of the operation. At the conclusion of the operation, UAS staff physically uploads the digital media evidence onto a thumb drive and physically impounds it in the property room, or digitally uploads the evidence onto the evidence.com system. After the transfer is complete the SD card is wiped.

All of the computers, thumb drives, recording devices, and SD cards used in this evidence collection, transfer, and impound process belong to the San Diego Police Department. No personally electronic devices are used in this procedure.

UPDATES, UPGRADES, AND CONFIGURATION CHANGES

In 2025 the UAS Unit procured an upgraded model of UAS to the DJI Matrice M30T. This new upgraded model is the DJI Matrice 4T. The Matrice 4T has all the same capabilities and features as the Matrice M30T. With this UAS Model upgrade, there are no changes to the video recording capabilities or procedures. The DJI Matrice 4T functions the same as the DJI Matrice M30T.

The DJI Matrice 4T was not used to support any law enforcement operations in 2025.

DEPLOYMENT LOCATION

Table of UAS deployment locations and utilization of Dejero DTS.

CATEGORY OF OPERATION	DEJERO DTS	DIVISION	AGENCY REQUEST
SWAT Support, High Risk Tactical Operation, or Suspect Search	NO	MIDCITY	SDPD
Crime Scene Evidence Collection	NO	NORTHERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	MIDCITY	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	SOUTHEASTERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	NO	CENTRAL	SDPD

CATEGORY OF OPERATION (continued)	DEJERO DTS	DIVISION	AGENCY REQUEST
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	OUT OF CITY	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	SOUTHERN	SDPD
Crime Scene Evidence Collection	NO	OUT OF CITY	SDSO
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	CENTRAL	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	MIDCITY	SDPD
Special Events (Enhanced Security)	YES	CENTRAL	SDPD
Special Events (Enhanced Security)	YES	CENTRAL	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	NO	EASTERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	NO	SOUTHERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	NO	WESTERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	NO	EASTERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	NO	NORTHEASTERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	NO	CENTRAL	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	MIDCITY	SDPD
SAR - Search and Rescue for Missing Persons and Photos	NO	NORTHWESTERN	SDPD
SAR - Search and Rescue for Missing Persons and Photos	NO	SOUTHEASTERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	NORTHERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	Yes	SOUTHERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	SOUTHEASTERN	SDPD
Crime Scene Evidence Collection	NO	EASTERN	SDPD
Civil Demonstrations and Civil Unrest	YES	CENTRAL	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	EASTERN	SDPD
Crime Scene Evidence Collection	NO	NORTHEASTERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	MIDCITY	SDPD

CATEGORY OF OPERATION (continued)	DEJERO DTS	DIVISION	AGENCY REQUEST
SAR - Search and Rescue for Missing Persons and Photos	NO	WESTERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	NO	NORTHEASTERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	MIDCITY	SDPD
SAR - Search and Rescue for Missing Persons and Photos	NO	WESTERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	MIDCITY	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	NO	SOUTHERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	NO	NORTHEASTERN	SDPD
Special Events (Enhanced Security)	YES	NORTHERN	SDPD
Special Events (Enhanced Security)	YES	NORTHERN	SDPD
Special Events (Enhanced Security)	YES	NORTHERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	NO	NORTHEASTERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	NORTHERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	NO	SOUTHEASTERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	CENTRAL	SDPD
SAR - Search and Rescue for Missing Persons and Photos	NO	OUT OF CITY	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	NO	CENTRAL	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	NO	SOUTHEASTERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	SOUTHERN	SDPD
Special Events (Enhanced Security)	YES	CENTRAL	SDPD
Special Events (Enhanced Security)	YES	CENTRAL	SDPD
Special Events (Enhanced Security)	YES	CENTRAL	SDPD
Special Events (Enhanced Security)	YES	CENTRAL	SDPD
Special Events (Enhanced Security)	YES	CENTRAL	SDPD
Special Events (Enhanced Security)	YES	WESTERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	MIDCITY	SDPD

CATEGORY OF OPERATION (continued)	DEJERO DTS	DIVISION	AGENCY REQUEST
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	SOUTHEASTERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	WESTERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	SOUTHERN	SDPD
Special Events (Enhanced Security)	YES	NORTHERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	NO	CENTRAL	SDPD
Special Events (Enhanced Security)	YES	NORTHERN	SDPD
Special Events (Enhanced Security)	YES	NORTHERN	SDPD
Special Events (Enhanced Security)	YES	NORTHERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	NO	CENTRAL	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	NO	EASTERN	SDPD
Crime Scene Evidence Collection	NO	EASTERN	SDPD
SAR - Search and Rescue for Missing Persons and Photos	NO	WESTERN	SDPD
Civil Demonstrations and Civil Unrest	YES	CENTRAL	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	SOUTHERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	OUT OF CITY	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	OUT OF CITY	SDPD
Special Events (Enhanced Security)	YES	CENTRAL	SDPD
Other (i.e. Inspections, Disaster Response, etc.)	YES	EASTERN	FAA/NTSB
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	OUT OF CITY	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	NO	CENTRAL	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	NORTHEASTERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	WESTERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	NO	WESTERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	MIDCITY	SDPD
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	SOUTHERN	SDPD

CATEGORY OF OPERATION (continued)	DEJERO DTS	DIVISION	AGENCY REQUEST
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	NORTHEASTERN	SDPD
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	NORTHERN	SDPD
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	SOUTHERN	SDPD
SWAT Support , High Risk Tactical Operation, or Suspect Search	NO	EASTERN	SDPD
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	SOUTHEASTERN	SDPD
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	EASTERN	SDPD
SAR - Search and Rescue for Missing Persons and Photos	NO	NORTHEASTERN	SDPD
SAR - Search and Rescue for Missing Persons and Photos	NO	NORTHEASTERN	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	OUT OF CITY	LMPD
SWAT Support , High Risk Tactical Operation, or Suspect Search	NO	NORTHEASTERN	SDPD
Civil Demonstrations and Civil Unrest	YES	EASTERN	SDPD
SWAT Support , High Risk Tactical Operation, or Suspect Search	NO	SOUTHEASTERN	SDPD
Crime Scene Evidence Collection	NO	WESTERN	SDPD
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	SOUTHEASTERN	SDPD
Special Events (Enhanced Security)	NO	NORTHWESTERN	SDPD
Special Events (Enhanced Security)	NO	NORTHWESTERN	SDPD
Special Events (Enhanced Security)	NO	NORTHWESTERN	SDPD
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	SOUTHEASTERN	SDPD
Special Events (Enhanced Security)	NO	NORTHWESTERN	SDPD
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	OUT OF CITY	SDPD
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	OUT OF CITY	SDPD
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	OUT OF CITY	SDPD
Crime Scene Evidence Collection	NO	OUT OF CITY	SDPD
Civil Demonstrations and Civil Unrest	YES	CENTRAL	SDPD
SWAT Support , High Risk Tactical Operation, or Suspect Search	NO	MIDCITY	SDPD

CATEGORY OF OPERATION (continued)	DEJERO DTS	DIVISION	AGENCY REQUEST
Civil Demonstrations and Civil Unrest	YES	CENTRAL	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	NO	SOUTHERN	SDPD
Special Events (Enhanced Security)	NO	NORTHWESTERN	SDPD
Special Events (Enhanced Security)	NO	NORTHWESTERN	SDPD
Special Events (Enhanced Security)	NO	NORTHWESTERN	SDPD
Special Events (Enhanced Security)	NO	NORTHWESTERN	SDPD
Civil Demonstrations and Civil Unrest	NO	CENTRAL	SDPD
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	CENTRAL	SDPD
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	OUT OF CITY	SDPD
SWAT Support, High Risk Tactical Operation, or Suspect Search	YES	OUT OF CITY	SDPD
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	OUT OF CITY	SDPD
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	OUT OF CITY	SDPD
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	MIDCITY	SDPD
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	SOUTHEASTERN	SDPD
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	SOUTHERN	SDPD
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	NORTHEASTERN	RIVERSIDE PD

COMMUNITY COMPLAINTS OR CONCERNS

The SDPD is committed to protecting the civil rights and liberties of our citizens as presented to the City Council for approval of these technologies. The SDPD has not received any complaints or concerns about these surveillance technologies and has not received any reports of disproportionate impacts. The Use Policies continue to protect civil rights and civil liberties.

AUDITS OR INVESTIGATIONS

In response to the Privacy Advisory Board's (PAB) Memorandum addressed to San Diego City Council President LaCava and Members of the San Diego City Council on April 17, 2025, which provided a request for more rigorous auditing processes, the SDPD's Research, Analysis, and Planning Division published Department Order (OR) 25-13 on April 25, 2025. This order requires the managing unit (the managing unit is the person(s) recognized as the subject matter expert (SME) for the Transparent and Responsible Use of Surveillance Technology ordinance reporting or who controls the equipment) to prepare for the required

Annual Report each year. The OR requires that the SMEs conduct quarterly audits of the equipment they are in charge of, including compiling and tracking information and data listed in SDMC 210.0102(a). On July 15, 2025, an additional Department Order, DO 25-23, was published. This DO requires Department members using any technology or database to enter a reference code/ID or justification for use of the technology or database with either a relevant full eight-digit case number, a full 11-digit event number, or other unique identification code. It requires that users no longer use nonspecific phrases or references and enhances the ability to audit the system.

In accordance with OR 25-13, and as an addition to the required quarterly audits by the managing unit, an independent audit was conducted by the Research, Analysis, and Planning Division (RAP)– Inspection and Control Unit. The audits were in addition to the quarterly audits required by the managing unit in OR 25-13. These audits targeted confirmation of the proper use of the technology, as stated in the Use Policy.

This technology was audited on 49 different case numbers, event numbers, or use statistics to verify the proper use of the technology. This included confirming a relevant identification number for the event and that the video recording(s) was impounded appropriately. No unauthorized uses of the technology were located during the audit conducted by RAP.

Any training issues or unintended input errors with this technology were identified and corrected. Continued errors or training issues will result in the user being suspended from the technology until they can be retrained on the technology.

Any substantial non-compliance or intentional misuse will be forwarded to the command or the Internal Affairs Unit for investigation and the subject may have their access permanently removed from the technology.

There was no unauthorized access of this technology and/or no located or reported violations of the Surveillance Use Policy or SDPD Policy or Procedure regarding this technology.

DATA BREACH OR UNAUTHORIZED ACCESS

The City of San Diego's Department of Information Technology and SDPD Information Technology Unit has identified no data breaches or unauthorized access to the data collected by the surveillance technology.

DATA BREACH DETECTION

The City's Department of Information Technology oversees the IT governance process and works with SDPD's Department of IT regarding project execution and risk assessment as well as selecting and approving technology solutions. Cyber security and technology risks are also assessed by the Department of IT. For additional details related to IT governance processes, refer to the information at the following link:

https://www.sandiego.gov/sites/default/files/fy23-fy27-it-strategic-plan-sd.pdf

INFORMATION AND STATISTICS

There are no direct relational crime statistics associated with or produced by the use of this technology.

Should the public want to access crime statistics for the City of San Diego, they can visit the City's *Crime Statistics & Crime Mapping* webpage: Crime Statistics & Crime Mapping | City of San Diego Official Website. The City's neighborhood crime summary dashboard is available

at: San Diego Neighborhood Crime Dashboard (arcgis.com). A tab on this dashboard, Crime Data Explorer, allows the user to query crimes specific to a City neighborhood.

Additionally, crime data is also available on the City's Open Data Portal: Datasets - City of San Diego Open Data Portal. This crime data can be downloaded into usable files; also available on this site are dictionaries to help navigate the different data sets.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

There were 21 Public Records Act requests regarding these surveillance technologies.

The information produced in response to these requests can be viewed on the City of San Diego's CPRA request portal: https://sandiego.nextrequest.com/

Request Number	Requested Date	Closed Date
25-8746	11/04/2025	11/28/2025
25-8670*	11/03/2025	11/04/2025
25-8669*	11/03/2025	11/04/2025
25-8667*	11/03/2025	11/04/2025
25-8666*	11/03/2025	11/04/2025
25-8665*	11/03/2025	11/04/2025
25-8664*	11/03/2025	11/04/2025
25-8332	10/22/2025	11/06/2025
25-8288	10/21/2025	12/11/2025
25-7838	10/06/2025	10/15/2025
25-7683	09/30/2025	Open
25-6948	09/06/2025	09/09/2025
25-6692	08/28/2026	11/06/2025
25-6409	08/20/2025	08/29/2025
25-6087	08/10/2025	10/14/2025
25-4868	06/26/2025	Open
25-4527	06/12/2025	06/13/2025
25-3842*	05/19/2025	05/29/2025
25-3841*	05/19/2025	05/29/2025
25-2880	04/14/2025	04/15/2025
25-1006	02/05/2025	02/11/2025

* Duplicate PRA

ANNUAL COST

During the 2025 Calendar year, the following funding sources supported procurement of SDPD UAS technology for new equipment and ongoing maintenance costs.

- City General funding supported $0.00.
- DOJ Seized Assets special funding source supported $9,280.51.
- California Seized Assets special funding source supported $18,886.71.
- SWAT Foundation funding supported $1,513.88.

During the 2025 Calendar year, the following funding sources supported procurement of Dejero DTS technology for new equipment and ongoing maintenance costs.

- City General funding supported $0.00.
- DOT Seized Assets special funding source supported $8,495.00.

- UASI Grant funding supported $149,069.69.

REQUESTED MODIFICATIONS TO THE USE POLICY

There were no requested modifications to this technology's Use Policy with regard to changes in operations or UAS capabilities.

There is a request to combine the multiple policies of the individual UAS makes and models into one all-encompassing policy that combines all of the already approved UAS features and capabilities to make one universal UAS policy.

San Diego Police Department
Covert Technologies

SDPD

ONE TEAM. ONE MISSION.

Department/Division: Police - Investigations II - Robbery

Related Policy/Procedure:

- **DP 3.02 –** Impound, Release, and Disposal of Property, Evidence, and Articles Missing Identification Marks
- **DP 3.26** – Media Evidence Recovery and Impounding/Preserving Procedures

DESCRIPTION

The San Diego Police Department utilizes the below listed audio/video recording equipment to create objective real-time recordings or to provide officer safety during covert investigative operations.

- **Covert Audio Recording Devices (Record Only)**: The Department utilizes covert audio recording devises (record only) to create objective real-time recordings. Audio obtained from this technology is used by the investigator requesting the equipment. Successfully recorded audio is maintained by the Detective for their investigation. The audio file will be attached to their investigation. The Covert Audio Recording Devices (Record Only) were utilized three times during the 2025 calendar year.

- **Covert Cloud Based Mobile Application**: The Department utilizes a covert cloud based mobile application (CBMA) and software for audiovisual recording, audio recording, GPS location, and recording of text/multimedia messages. A CBMA is designed to create objective real-time recordings and documentation to develop and further investigations, and to protect undercover operators at risk during sensitive investigations. CBMA devices are generally utilized through a phone line. The department utilizes 150 different phone lines and has 75 available video lines. There were 40,210 uses of this technology for 2025.

- **PTZ Cloud Based System**: The Department utilizes Pan/Tilt/Zoom (PTZ) video camera recorders internally and transmit the video data to a cloud-based server. The purpose is to create objective real-time video recordings to develop and further investigations. The PTZ camera capabilities are valuable when conditions change while the equipment has been deployed and the camera can be adjusted for those changes. The device is used in areas where there are repeat offenses and/or more evidence is needed for a successful apprehension of a suspect. This technology was not utilized during the 2025 calendar year.

- **Trail Cameras**: The Department utilizes battery powered motion activated “trail” cameras. These cameras are used when normal power sources for other equipment is unavailable. This device is used in areas where there are repeat offenses and/or more evidence is needed for the successful apprehension a suspect. This technology was utilized three times during the 2025 calendar year.

- **PTZ Video Camera Mobile Units**: The Department utilizes Pan/Tilt/Zoom (PTZ) video cameras with recorders to create objective real-time video recordings to develop and further investigations. The PTZ camera capabilities are valuable when conditions change while the equipment has been deployed and the camera can be adjusted for

those changes. The device is used in areas where there are repeat offenses and/or more evidence is needed for the successful apprehension of a suspect. The system was utilized eight times during the third quarter of the calendar year 2025.

- **Power Over Ethernet (POE) Digital Video Recorder and Cameras**: The Department utilizes power over ethernet digital video recorders (POE/DVR and POE/NVR) to create objective real-time recordings to develop and further investigations. The systems use PTZ (Pan-Tilt-Zoom) cameras and fixed cameras. These systems are used in areas where there are repeat offenses and/or more evidence needs to be collected for a successful apprehension of a suspect. The cameras utilized within this technology include POE Digital Video Cameras, POE Network Video Cameras, POE Video Cameras, and PTZ Video Cameras. All of the cameras will not operate without the Digital Video Recorder (DVR) or the Network Video Recorder (NVR). This technology was utilized three times during the 2025 calendar year.

- **Covert Audio Recording Devices (Remote Listening Capable)**: The Department utilizes covert audio recording devices (remote listening capable) to create objective real-time recordings and to protect undercover operators at risk during sensitive operations. The covert audio recording devices with remote listening capability currently in the Department's inventory are outdated and no longer in use. They are not functional and were not utilized during the 2025 calendar year. The Department is currently researching modern equipment with the same capability to replace the existing non-functional technology.

- **Covert Audio/Visual Recording Devices**: The Department utilizes covert audio recording devices to create objective real-time recordings and to protect undercover operators at risk during sensitive operations. This technology was not utilized during the 2025 calendar year.

SHARING OF DATA

Audio and/or video obtained from this technology is used by the Detective requesting the equipment. Successfully recorded audio and/or video recorded is maintained by the Detective for their investigation and records of the release of this information are not retained by the managing unit.

Recorded files may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes, which includes criminal investigations and prosecution, as allowed by law. The recorded files were not used in immigration enforcement.

LOCATION

These devices are used in undercover operations based on information the detective has obtained during their investigation. The devices have been used in locations which are based on those investigations and are placed at specific locations to watch specific targets.

UPDATES, UPGRADES, AND CONFIGURATION CHANGES

The Power Over the Ethernet Digital Video Recorder and Camera equipment were reconfigured with software updates from the manufacturer. These devices record audio files to hard drive space on the unit. The devices have been updated, with no change to the

functionality of the unit. There were no fees attached to the updates recommended by the manufacturer.

The department added two more NVR's that are Trade Agreements Act (TAA) and National Defense Authorization Act (NDAA) complaint to allow real-time access during use of POE fixed and PTZ camera systems. These systems require a modem or a cellular hotspot to be utilized for real-time remote access.

DEPLOYMENT LOCATION

This technology was utilized in all the San Diego Police Department service areas. Most locations are confidential.

COMMUNITY COMPLAINTS OR CONCERNS

The Department is committed to protecting civil rights and liberties of all citizens as presented to the City Council prior to the approval of this technology. The Department did not receive any complaints or concerns regarding this surveillance technology or receive any reports of disproportionate impacts. The Use Policy protected civil rights and liberties.

AUDITS OR INVESTIGATIONS

In response to the Privacy Advisory Board's (PAB) Memorandum addressed to San Diego City Council President LaCava and Members of the San Diego City Council on April 17, 2025, which provided a request for more rigorous auditing processes, the SDPD's Research, Analysis, and Planning Division published Department Order (OR) 25-13 on April 25, 2025. This order requires the managing unit (the managing unit is the person(s) recognized as the subject matter expert (SME) for the Transparent and Responsible Use of Surveillance Technology ordinance reporting or who controls the equipment) to prepare for the required Annual Report each year. The OR requires that the SMEs conduct quarterly audits of the equipment they are in charge of, including compiling and tracking information and data listed in SDMC 210.0102(a). On July 15, 2025, an additional Department Order, DO 25-23, was published. This DO requires Department members using any technology or database to enter a reference code/ID or justification for use of the technology or database with either a relevant full eight-digit case number, a full 11-digit event number, or other unique identification code. It requires that users no longer use nonspecific phrases or references and enhances the ability to audit the system.

In accordance with OR 25-13, and as an addition to the required quarterly audits by the managing unit, an independent audit was conducted by the Research, Analysis, and Planning Division (RAP)– Inspection and Control Unit. The audits were in addition to the quarterly audits required by the managing unit in OR 25-13. These audits targeted confirmation of the proper use of the technology, as stated in the Use Policy.

This technology was audited on different case numbers, event numbers, or use statistics to verify the proper use of the technology. This included confirming a relevant identification number for the event and that the video recording(s) was impounded appropriately.

- **Covert Audio Recording Devices (Record Only)**: The Covert Audio Recording Devices (Record Only) were utilized three times during the 2025 calendar year. RAP conducted an audit on all three uses.

- **Covert Cloud Based Mobile Application**: CBMA devices are generally utilized through a phone line. The department utilizes 150 different phone lines and has 75 available video lines. There were 40,210 uses of this technology for 2025. This technology is utilized after supervisory approval of an investigation. Its use is monitored by a supervisor to verify the proper use of the technology. No unauthorized uses of the technology were located during the audit conducted by RAP.

- **PTZ Cloud Based System**: This technology was not utilized during the 2025 calendar year. No Audits were conducted due to the lack of use on this equipment.

- **Trail Cameras**: This technology was utilized three times during the 2025 calendar year. RAP conducted an audit on all three uses.

- **PTZ Video Camera Mobile Units**: The system was utilized eight times during the third quarter of the calendar year 2025. RAP conducted an audit on all eight uses.

- **Power Over Ethernet (POE) Digital Video Recorder and Cameras**: This technology was utilized three times during the 2025 calendar year. RAP conducted an audit on all three uses.

- **Covert Audio Recording Devices (Remote Listening Capable)**: This technology is not functional and was not utilized during the 2025 calendar year. No audit was conducted.

- **Covert Audio/Visual Recording Devices**: This technology was not utilized during the 2025 calendar year. No audit was conducted.

No unauthorized uses of the technology were located during the audit conducted by RAP.

Any training issues or unintended input errors with this technology were identified and corrected. Continued errors or training issues will result in the user being suspended from the technology until they can be retrained on the technology.

Any substantial non-compliance or intentional misuse will be forwarded to the command or the Internal Affairs Unit for investigation and the subject may have their access permanently removed from the technology.

There was no unauthorized access of this technology and/or no located or reported violations of the Surveillance Use Policy or SDPD Policy or Procedure regarding this technology.

DATA BREACH OR UNAUTHORIZED ACCESS

The City of San Diego's Department of Information Technology and SDPD Information Technology Unit has identified no data breaches or unauthorized access to the data collected by the surveillance technology.

DATA BREACH DETECTION

The City's Department of Information Technology oversees the IT governance process and works with SDPD's Department of IT regarding project execution and risk assessment as well as selecting and approving technology solutions. Cyber security and technology risks are also assessed by the Department of IT. For additional details related to IT governance processes, refer to the information at the following link:

https://www.sandiego.gov/sites/default/files/fy23-fy27-it-strategic-plan-sd.pdf

INFORMATION AND STATISTICS

There are no direct relational crime statistics associated with or produced by the use of this technology.

Should the public want to access crime statistics for the City of San Diego, they can visit the City's *Crime Statistics & Crime Mapping* webpage: Crime Statistics & Crime Mapping | City of San Diego Official Website. The City's neighborhood crime summary dashboard is available at: San Diego Neighborhood Crime Dashboard (arcgis.com). A tab on this dashboard, Crime Data Explorer, allows the user to query crimes specific to a City neighborhood.

Additionally, crime data is also available on the City's Open Data Portal: Datasets - City of San Diego Open Data Portal. This crime data can be downloaded into usable files; also available on this site are dictionaries to help navigate the different data sets.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

The information produced in response to these requests can be viewed on the City of San Diego's CPRA request portal: https://sandiego.nextrequest.com/

REQUEST NUMBER	REQUEST DATE	CLOSED DATE
25-7858	10/07/2025	11/02/2025

ANNUAL COST

Covert Audio Recording Devices (Record Only): The units were a one-time fee to purchase. The units record to a hard drive on each individual unit. The units do not use or have access to a cloud system. There are no service fees for these devices other than the original purchase price.

Covert Cloud Based Mobile Application: The cost for this service is $28,985.00 a year.

PTZ Cloud Based System: There will be a cost for a cell phone SIM card when the device is put into use.

Trail Cameras: The units were a one-time fee to purchase. There are no annual costs for this technology.

PTZ Video Camera Mobile Units: There will be a cost for a cell phone SIM card when the device is put into use.

Power Over Ethernet (POE) Digital Video Recorder and Cameras: Two of the systems have remote viewing, which need a cell phone SIM card. There are no other costs to run these systems.

Covert Audio Recording Devices (Remote Listening Capable): Not currently in use.

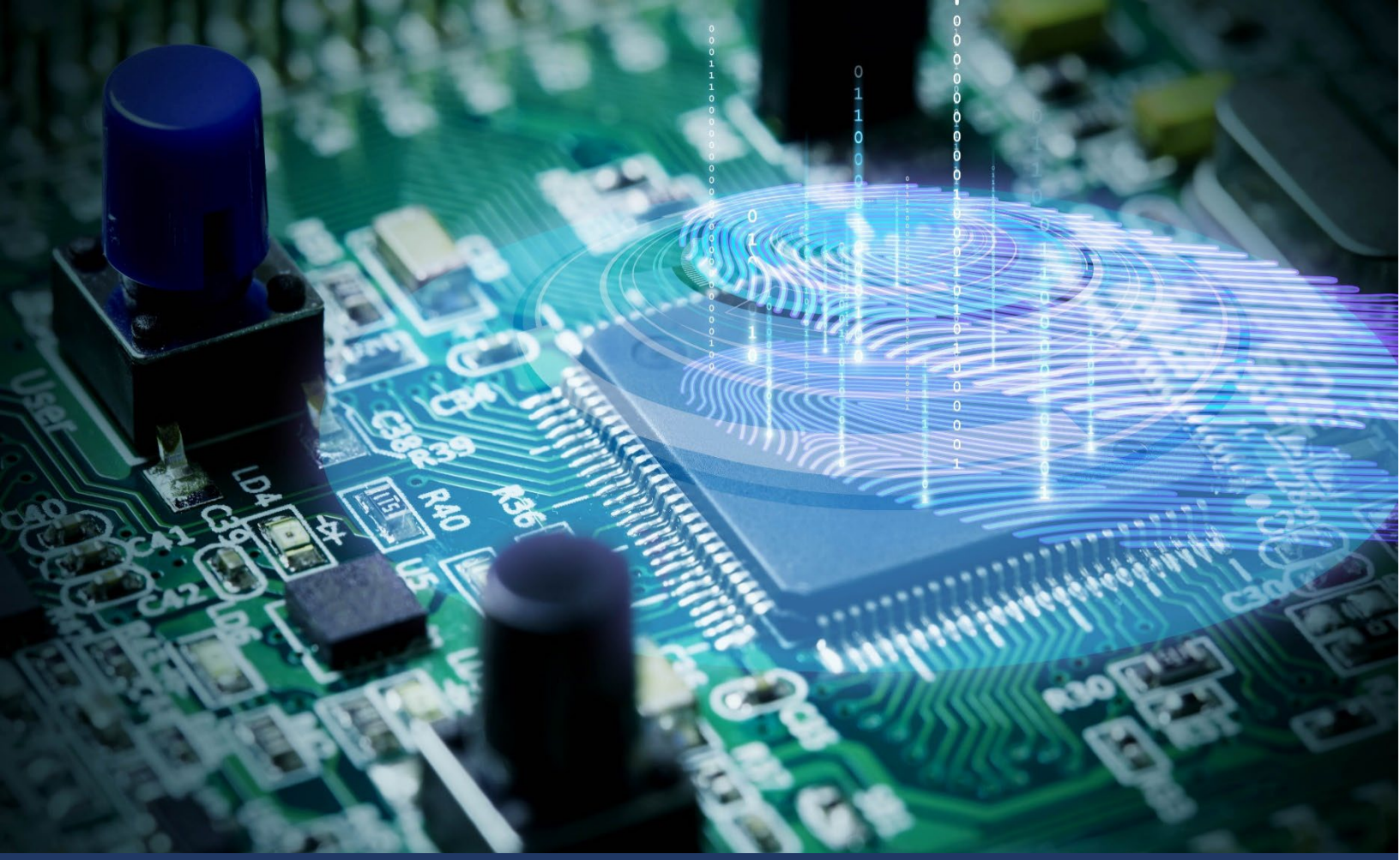
Covert Audio/Video Recording Devices: The devices were a one-time fee to purchase. There are no annual costs for this technology.

There were no independent personnel costs outside of the normal course of the operators' duties.

The funding for these technologies was provided by a JAG Grant.

REQUESTED MODIFICATIONS TO THE USE POLICY

There are no requested modifications to these technologies' Use Policies.



San Diego Police Department Device Forensic Technologies

SDPD

ONE TEAM. ONE MISSION.

San Diego Police Department

Mobile Device Forensic Technologies

Department/Division: Police - Crime Laboratory

Related Policy/Procedure:

- **DP 1.45** -Use of City/Department Computer System
- **DP 3.02** -Impound, Release, and Disposal of Property, Evidence, and Articled Missing Identification Marks
- **DP 3.26 –** Media Evidence Recovery and Impounding/Preserving

---

DESCRIPTION

The San Diego Police Department (SDPD) Crime Laboratory is one of the few laboratories in the country with an accredited Forensic Technology Unit (FTU) staffed by civilian personnel. FTU's mission is to provide SDPD and the citizens of San Diego with comprehensive, impartial, reliable, accurate, and timely scientific analysis of evidence by experts skilled in the latest mobile device forensic technologies.

"Mobile device forensic technologies" (MDFT) is a generic term describing the tools which are used to extract and analyze data from mobile devices (such as cell phones) and generate/review reports from that extracted data. The MDFT currently utilized by the SDPD are the Cellebrite Inseyets tool suite (Cellebrite), Magnet Axiom (Axiom), and Magnet Graykey (Graykey).

SDPD utilizes MDFT only when proper legal authority is obtained. Only those that have been trained and certified by FTU are authorized to use MDFT. All new users must be manually authorized and enabled by FTU before being given access to the tools.

The Cellebrite and Graykey tools are designed to complete extractions without altering any of the data or adding data to the phone. Due to the large variety of mobile device models and manufacturers, not all mobile devices can be extracted; both tools are utilized because different tools support different types of devices. The Cellebrite and Graykey tools can also extract data that has been deleted or hidden.

Once the data is extracted, the Cellebrite and Axiom tools are used to categorize and analyze extracted data, then generate reports for assigned investigators to review. Both tools are often used together because each tool interprets the extracted data differently; the resulting reports typically supplement each other.

Extracted data is stored in user-specific secure folders on SDPD networks; only the user who extracted the data has access to it. The resulting report(s) generated from extracted data are only shared with those who have obtained proper legal authority to review those report(s). The SDPD networks that store this data are managed by the FTU and IT/Data Systems analysts.

Approximately 71 terabytes (TB) of data was generated via MDFT in 2025, impacting over 200 investigations through the forensic extraction of approximately 292 evidentiary mobile devices.

SHARING OF DATA

Data was only shared according to the approved Use Policies. The resulting report(s) generated from extracted data are only shared with those who have obtained proper legal authority to review those report(s). Proper legal authority is defined by the California Electronic Communications Privacy Act [ECPA; SB 178 (2016) codified in California Penal Code 1546.1]. A copy of the data extracted using MDFT is retained by the investigator and the Crime Laboratory does not receive information on whether the extracted data is shared outside of the City of San Diego.

Data that has been extracted using MDFT is not shared with external sources without a court order or other legal proceedings, such as for prosecution or discovery. The extracted data is considered confidential, and there is no third-party access or sharing. Vendors do not have access to the extracted data.

LOCATION

The MDFT are only installed on SDPD systems and utilized on evidentiary mobile devices according to the approved Use Policies.

UPDATES, UPGRADES, AND CONFIGURATION CHANGES

Software updates typically provide support for additional mobile device models, applications, operating systems, and/or enhance performance of the tools. Installing software updates allows SDPD to investigate more types of evidentiary mobile devices and/or the data stored on them. The following software updates were installed on the MDFT:

Cellebrite Inseyets UFED	Cellebrite Inseyets Physical Analyzer	Magnet Axiom	Magnet Graykey
10.4.1.147	10.4.1.2071	8.9.0.43012	1.25.0.30192015 / 5.7.0b2.30381457
10.5.0.222	10.5.0.1016	8.9.1.43258	1.25.0.30192015 / 5.8.0.30651334
10.5.0.368	10.5.0.1027	9.0.0.43519	1.26.0.30651434 / 5.8.1.30661541
10.6.1.604	10.6.0.3094	9.1.0.43876	1.26.0.30651434 / 5.9.0.30790104
10.7.0.181	10.6.1.3005	9.2.0.44134	1.26.0.30651434 / 5.10.1.30941822
	10.7.1.5013	9.4.1.45125	1.26.0.30651434 / 5.11.0b0.31020103
		9.5.0.45393	1.26.0.30651434 / 5.11.0b2.31080104
		9.8.0.46347	1.26.0.30651434 / 5.11.0.31081726
			1.26.0.30651434 / 5.12.0b0.31140804
			1.26.0.30651434 / 5.12.0b2.31191604
			1.26.0.30651434 / 6.0.1.31361955
			1.26.2.31231301 / 6.1.0.31592321
			1.26.3.31482045 / 6.2.0b1.31710003
			1.26.4.31852311 / 6.4.0b4.32161248
			1.26.6.32401155 / 6.6.0b0.32460803
			1.26.6.32401155 / 6.6.0.32602003
			1.26.6.32401155 / 6.7.0b3.32691603
			1.26.6.32401155 / 6.7.0b4.32732044
			1.26.6.32401155 / 6.7.0.32761202
			1.26.6.32401155 / 6.8.0b2.32822050

Cellebrite Inseyets UFED (continued)	Cellebrite Inseyets Physical Analyzer (continued)	Magnet Axiom (continued)	Magnet Graykey (continued)
			1.26.6.32401155 / 6.8.0b8.32951330
			1.26.6.32401155 / 6.8.0.32971231
			1.26.6.32401155 / 6.9.0b0.32982003
			1.26.6.32401155 / 6.9.0b1.33030049
			1.27.0.32901420 / 6.9.0b3.33090004
			1.27.0.32901420 / 7.0.0.33162004
			1.27.0.32901420 / 7.1.0b3.33261411
			1.27.0.32901420 / 7.1.0b5.33331604
			1.27.2.33361518 / 7.1.0.33442352
			1.27.3.33591653 / 7.2.1.33641640

DEPLOYMENT LOCATION

The MDFT are only deployed in secure SDPD facilities.

COMMUNITY COMPLAINTS OR CONCERNS

The Department is committed to protecting civil rights and liberties of our citizens as presented to the City Council prior to approval of this technology. The Department has not received any complaints or concerns about this surveillance technology or received any reports of disproportionate impacts. The Use Policy continues to protect civil rights and civil liberties.

AUDITS OR INVESTIGATIONS

In response to the Privacy Advisory Board's (PAB) Memorandum addressed to San Diego City Council President LaCava and Members of the San Diego City Council on April 17, 2025, which provided a request for more rigorous auditing processes, the SDPD's Research, Analysis, and Planning Division published Department Order (OR) 25-13 on April 25, 2025. This order requires the managing unit (the managing unit is the person(s) recognized as the subject matter expert (SME) for the Transparent and Responsible Use of Surveillance Technology ordinance reporting or who controls the equipment) to prepare for the required Annual Report each year. The OR requires that the SMEs conduct quarterly audits of the equipment they are in charge of, including compiling and tracking information and data listed in SDMC 210.0102(a). On July 15, 2025, an additional Department Order, DO 25-23, was published. This DO requires Department members using any technology or database to enter a reference code/ID or justification for use of the technology or database with either a relevant full eight-digit case number, a full 11-digit event number, or other unique identification code. It requires that users no longer use nonspecific phrases or references and enhances the ability to audit the system.

In accordance with OR 25-13, and as an addition to the required quarterly audits by the managing unit, an independent audit was conducted by the Research, Analysis, and Planning Division (RAP)– Inspection and Control Unit. The audits were in addition to the quarterly audits required by the managing unit in OR 25-13. These audits targeted confirmation of the proper use of the technology, as stated in the Use Policy.

These three technologies were each audited on 12 different case numbers event numbers, or use statistics to verify the proper use of the technology. No unauthorized uses of the technology were located during the audit conducted by RAP.

Any training issues or unintended input errors with this technology were identified and corrected. Continued errors or training issues will result in the user being suspended from the technology until they can be retrained on the technology.

Any substantial non-compliance or intentional misuse will be forwarded to the command or the Internal Affairs Unit for investigation and the subject may have their access permanently removed from the technology.

There was no unauthorized access of this technology and/or no located or reported violations of the Surveillance Use Policy or SDPD Policy or Procedure regarding this technology.

DATA BREACH OR UNAUTHORIZED ACCESS

The City of San Diego's Department of Information Technology and SDPD Information Technology Unit has identified no data breaches or unauthorized access to the data collected by the surveillance technology.

DATA BREACH DETECTION

The City's Department of Information Technology oversees the IT governance process and works with SDPD's Department of IT regarding project execution and risk assessment as well as selecting and approving technology solutions. Cyber security and technology risks are also assessed by the Department of IT. For additional details related to IT governance processes, refer to the information at the following link:

https://www.sandiego.gov/sites/default/files/fy23-fy27-it-strategic-plan-sd.pdf

FTU and IT/Data Systems are the administrators of the mobile device extraction networks. Network security is monitored on a daily basis for unauthorized activity, and regular maintenance is performed.

Key card access logs are reviewed annually.

Each use of the MDFT is reviewed by FTU.

INFORMATION AND STATISTICS

There are no direct relational crime statistics associated with or produced by the use of this technology.

Should the public want to access crime statistics for the City of San Diego, they can visit the City's *Crime Statistics & Crime Mapping* webpage: Crime Statistics & Crime Mapping | City of San Diego Official Website. The City's neighborhood crime summary dashboard is available at: San Diego Neighborhood Crime Dashboard (arcgis.com). A tab on this dashboard, Crime Data Explorer, allows the user to query crimes specific to a City neighborhood.

Additionally, crime data is also available on the City's Open Data Portal: Datasets - City of San Diego Open Data Portal. This crime data can be downloaded into usable files; also available on this site are dictionaries to help navigate the different data sets.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

The information produced in response to these requests can be viewed on the City of San Diego's CPRA request portal: https://sandiego.nextrequest.com/

REQUEST NUMBER	REQUEST DATE	CLOSED DATE
25-7858	10/07/2025	11/02/2025

ANNUAL COST

The approximate costs of the MDFT for 2025 total $211,310.03 and will be paid via the General Fund. The cost per technology is listed below:

- Cellebrite Inseyets: $162,365.03
- Magnet Graykey: $33,105
- Magnet Axiom: $15,840

The approximate costs of the MDFT for 2026 total $X and will be paid via the General Fund. The cost per technology is listed below:

- Cellebrite Inseyets: $189,000
- Magnet Graykey: $61,395
- Magnet Axiom: $28,900

REQUESTED MODIFICATIONS TO THE USE POLICY

No modifications to the Use Policies are requested.

San Diego Police Department Emergency Negotiations

SDPD

ONE TEAM. ONE MISSION.

San Diego Police Department

Tactical Throw Phone and Commander II

Department/Division: Police - Emergency Negotiations Team

Related Policy/Procedure:

- DP 8.14 - Incidents Involving Hostage/Emergency Negotiations

DESCRIPTION

The 836 Technologies CINT Commander II and Tactical Throw Phone are utilized by the San Diego Police Department Emergency Negotiations Team during critical / crisis incidents involving life-threatening behavior. The equipment aids crisis negotiators in communicating with involved parties, suspects and hostages, to assist in efforts to bring these potential life-threatening incidents to a peaceful resolution.

The 836 Technologies CINT Commander II was used four times during the 2025 calendar year. The 836 Technologies Tactical Throw Phone was not utilized during the 2025 Calendar year.

SHARING OF DATA

Data was acquired four times by 836 Technologies CINT Commander II, during the 2025 calendar year. No Data acquired by the 836 Technologies CINT Commander II has been shared. There was no data acquired by the 836 Technologies Tactical Throw Phone.

LOCATION

The 836 Technologies CINT Commander II was used within the mobile command vehicle to communicate, via phone, with individuals during critical / crisis incidents involving life-threatening behavior during the 2025 calendar year.

UPDATES, UPGRADES, AND CONFIGURATION CHANGES

There were no alterations, upgrades or system reconfigurations to the 836 Technologies CINT Commander II and Tactical Throw Phone during the 2025 calendar year.

DEPLOYMENT LOCATION

The 836 Technologies CINT Commander II was utilized at the following locations during the 2025 calendar year.

LOCATION	DIVISION
2000 Via Casa Alta	NORTHERN
4200 Voltaire Street	WESTERN
2100 Front Street	CENTRAL
4100 Voltaire Street	WESTERN

The 836 Technologies Tactical Throw Phone was not utilized during the 2025 calendar year.

COMMUNITY COMPLAINTS OR CONCERNS

The SDPD is committed to protecting the civil rights and liberties of our citizens as presented to the City Council for approval of these technologies. The SDPD has not received any complaints or concerns about these surveillance technologies and has not received any reports of disproportionate impacts. The Use Policies continue to protect civil rights and civil liberties.

The Department has not received any complaints or concerns about this surveillance technology.

AUDITS OR INVESTIGATIONS

In response to the Privacy Advisory Board's (PAB) Memorandum addressed to San Diego City Council President LaCava and Members of the San Diego City Council on April 17, 2025, which provided a request for more rigorous auditing processes, the SDPD's Research, Analysis, and Planning Division published Department Order (OR) 25-13 on April 25, 2025. This order requires the managing unit (the managing unit is the person(s) recognized as the subject matter expert (SME) for the Transparent and Responsible Use of Surveillance Technology ordinance reporting or who controls the equipment) to prepare for the required Annual Report each year. The OR requires that the SMEs conduct quarterly audits of the equipment they are in charge of, including compiling and tracking information and data listed in SDMC 210.0102(a). On July 15, 2025, an additional Department Order, DO 25-23, was published. This DO requires Department members using any technology or database to enter a reference code/ID or justification for use of the technology or database with either a relevant full eight-digit case number, a full 11-digit event number, or other unique identification code. It requires that users no longer use nonspecific phrases or references and enhances the ability to audit the system.

In accordance with OR 25-13, and as an addition to the required quarterly audits by the managing unit, an independent audit was conducted by the Research, Analysis, and Planning Division (RAP)– Inspection and Control Unit. The audits were in addition to the quarterly audits required by the managing unit in OR 25-13. These audits targeted confirmation of the proper use of the technology, as stated in the Use Policy.

The 836 Technologies CINT Commander II technology was audited on 4 different case numbers, event numbers, or use statistics to verify the proper use of the technology. The 836 Technologies Tactical Throw Phone was not utilized during the 2025 Calendar year, so no audit was conducted. No unauthorized uses of the technology were located during the audit conducted by RAP.

Any training issues or unintended input errors with this technology were identified and corrected. Continued errors or training issues will result in the user being suspended from the technology until they can be retrained on the technology.

Any substantial non-compliance or intentional misuse will be forwarded to the command or the Internal Affairs Unit for investigation and the subject may have their access permanently removed from the technology.

There was no unauthorized access of this technology and/or no located or reported violations of the Surveillance Use Policy or SDPD Policy or Procedure regarding this technology.

DATA BREACH OR UNAUTHORIZED ACCESS

The City of San Diego's Department of Information Technology and SDPD Information Technology Unit has identified no data breaches or unauthorized access to the data collected by the surveillance technology.

DATA BREACH DETECTION

The City's Department of Information Technology oversees the IT governance process and works with SDPD's Department of IT regarding project execution and risk assessment as well as selecting and approving technology solutions. Cyber security and technology risks are also assessed by the Department of IT. For additional details related to IT governance processes, refer to the information at the following link:

https://www.sandiego.gov/sites/default/files/fy23-fy27-it-strategic-plan-sd.pdf

INFORMATION AND STATISTICS

There are no direct relational crime statistics associated with or produced by the use of this technology.

Should the public want to access crime statistics for the City of San Diego, they can visit the City's *Crime Statistics & Crime Mapping* webpage: Crime Statistics & Crime Mapping | City of San Diego Official Website. The City's neighborhood crime summary dashboard is available at: San Diego Neighborhood Crime Dashboard (arcgis.com). A tab on this dashboard, Crime Data Explorer, allows the user to query crimes specific to a City neighborhood.

Additionally, crime data is also available on the City's Open Data Portal: Datasets - City of San Diego Open Data Portal. This crime data can be downloaded into usable files; also available on this site are dictionaries to help navigate the different data sets.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

The information produced in response to these requests can be viewed on the City of San Diego's CPRA request portal: https://sandiego.nextrequest.com/

REQUEST NUMBER	REQUEST DATE	CLOSED DATE
25-7858	10/07/2025	11/02/2025

ANNUAL COST

There were no associated costs for the use of the 836 Technologies CINT Commander II and Tactical Throw Phone during the 2025 calendar year.

REQUESTED MODIFICATIONS TO THE USE POLICY

There are no requested modifications to this technology's Use Policy.

San Diego Police Department Investigative Tools

SDPD

ONE TEAM. ONE MISSION.

Department/Division: Police - Traffic Investigations Unit (TIU)

Related Policy/Procedure:

- DP 3.26 – Media Evidence Recovery and Impounding-Preserving Procedures

---

DESCRIPTION

The Berla equipment is used after a crime has been committed and an involved vehicle is located and recovered. Use of the Berla equipment requires a valid warrant or consent from the vehicle's owner. An authorized user will attempt to acquire and then analyze data from the involved vehicle. The equipment is used by sworn peace officers who are trained and/or certified by Berla.

A log is kept of those investigators that have requested a Berla analysis. The operator of the Berla is also logged. Use of the Berla equipment requires a valid warrant or consent from the vehicle's owner.

The Berla equipment was used ten times in 2025.

SHARING OF DATA

Each of the ten uses of the Berla equipment in 2025 was in relation to a felony criminal investigation. The information obtained during the search was therefore included as evidence and provided to the requesting Detective. If the case resulted in prosecution, the Detective would be required to provide the data to the prosecuting attorney. This would also require the data be provided to the defense attorney through the discovery process.

All ten uses were for criminal investigations conducted by SDPD. No uses involved agencies outside the SDPD.

LOCATION

The Berla equipment is kept in a locked cabinet at SDPD and access is limited to authorized sworn personnel. The computer storing the Berla software is password protected and only authorized users may access it.

UPDATES, UPGRADES, AND CONFIGURATION CHANGES

In 2025, Berla issued four software updates:

- 4.7 – Expanded support for Hyundai and Kia vehicles
- 4.12 – Added support for Genesis vehicles
- 4.13 – Expanded support for Toyota and Genesis vehicles
- 4.14 – Added support for Subaru vehicles and expanded support for GM and BMW vehicles.

DEPLOYMENT LOCATION

Use of the Bela equipment is typically done on vehicles that were impounded as evidence and stored at SDPD Traffic Division; therefore, the equipment does not usually get deployed to outside locations.

COMMUNITY COMPLAINTS OR CONCERNS

The Department is committed to protecting civil rights and liberties of our citizens as presented to the City Council prior to approval of this technology. The Department has not received any complaints or concerns about this surveillance technology or received any reports of disproportionate impacts. The Use Policy remains adequate to protect civil rights and civil liberties.

AUDITS OR INVESTIGATIONS

In response to the Privacy Advisory Board's (PAB) Memorandum addressed to San Diego City Council President LaCava and Members of the San Diego City Council on April 17, 2025, which provided a request for more rigorous auditing processes, the SDPD's Research, Analysis, and Planning Division published Department Order (OR) 25-13 on April 25, 2025. This order requires the managing unit (the managing unit is the person(s) recognized as the subject matter expert (SME) for the Transparent and Responsible Use of Surveillance Technology ordinance reporting or who controls the equipment) to prepare for the required Annual Report each year. The OR requires that the SMEs conduct quarterly audits of the equipment they are in charge of, including compiling and tracking information and data listed in SDMC 210.0102(a). On July 15, 2025, an additional Department Order, DO 25-23, was published. This DO requires Department members using any technology or database to enter a reference code/ID or justification for use of the technology or database with either a relevant full eight-digit case number, a full 11-digit event number, or other unique identification code. It requires that users no longer use nonspecific phrases or references and enhances the ability to audit the system.

In accordance with OR 25-13, and as an addition to the required quarterly audits by the managing unit, an independent audit was conducted by the Research, Analysis, and Planning Division (RAP)– Inspection and Control Unit. The audits were in addition to the quarterly audits required by the managing unit in OR 25-13. These audits targeted confirmation of the proper use of the technology, as stated in the Use Policy.

This technology was audited on 10 different case numbers, event numbers, or use statistics to verify the proper use of the technology. No unauthorized uses of the technology were located during the audit conducted by RAP.

Any training issues or unintended input errors with this technology were identified and corrected. Continued errors or training issues will result in the user being suspended from the technology until they can be retrained on the technology.

Any substantial non-compliance or intentional misuse will be forwarded to the command or the Internal Affairs Unit for investigation and the subject may have their access permanently removed from the technology.

There was no unauthorized access of this technology and/or no located or reported violations of the Surveillance Use Policy or SDPD Policy or Procedure regarding this technology.

DATA BREACH OR UNAUTHORIZED ACCESS

The City of San Diego's Department of Information Technology and SDPD Information Technology Unit has identified no data breaches or unauthorized access to the data collected by the surveillance technology.

DATA BREACH DETECTION

The City's Department of Information Technology oversees the IT governance process and works with SDPD's Department of IT regarding project execution and risk assessment as well as selecting and approving technology solutions. Cyber security and technology risks are also assessed by the Department of IT. For additional details related to IT governance processes, refer to the information at the following link:

https://www.sandiego.gov/sites/default/files/fy23-fy27-it-strategic-plan-sd.pdf

The Berla equipment is not connected to a network. To date, there have been no data breaches relayed to users from Berla or identified by the managing unit.

INFORMATION AND STATISTICS

There are no direct relational crime statistics associated with or produced by the use of this technology.

Should the public want to access crime statistics for the City of San Diego, they can visit the City's *Crime Statistics & Crime Mapping* webpage: Crime Statistics & Crime Mapping | City of San Diego Official Website. The City's neighborhood crime summary dashboard is available at: San Diego Neighborhood Crime Dashboard (arcgis.com). A tab on this dashboard, Crime Data Explorer, allows the user to query crimes specific to a City neighborhood.

Additionally, crime data is also available on the City's Open Data Portal: Datasets - City of San Diego Open Data Portal. This crime data can be downloaded into usable files; also available on this site are dictionaries to help navigate the different data sets.

Of the ten uses of the Berla equipment in 2025, one was for a murder investigation, three were for DUI murder and/or manslaughter investigations, one was for a felony hit and run investigation, one was for a fatal traffic collision investigation, and four were for felony theft and/or burglary investigations.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

The information produced in response to these requests can be viewed on the City of San Diego's CPRA request portal: https://sandiego.nextrequest.com/

REQUEST NUMBER	REQUEST DATE	CLOSED DATE
25-7858	10/07/2025	11/02/2025

ANNUAL COST

The annual software renewal fee for the Berla technology is $3,250 and is funded through the General Fund.

REQUESTED MODIFICATIONS TO THE USE POLICY

There are no requested modifications to this technology's Use Policy.

San Diego Police Department

Cellhawk

Department/Division: Police - Crime Analysis Unit

Related Policy/Procedure:

- DP 1.45 - Use of City/Department Computer Systems
- DP 4.13 - Non-Official or Personal Custody of Records/Files/Recordings Policy

---

DESCRIPTION

CellHawk is specialized mapping software that is used in investigations to visualize location-based data for analysis in cases typically involving cell phones. Detectives and Crime Analysts utilize CellHawk's symbolized visualization of this type of data to determine the general or specific whereabouts of a cell phone, which may inform an investigation.

In 2025, Cellhawk was used in 242 cases.

SHARING OF DATA

Data is not acquired through the use of CellHawk, as it is merely specialized mapping software used to visually represent location-based files that are uploaded into the system.

Uploaded files can be viewed by either Detectives or Crime Analysts that upload files into the system, sometimes working in conjunction with one another on an investigation.

Additionally, files retained in the system can be accessed by CellHawk analysts. Typically, the scenario in which this would happen involves the user (Detective or Crime Analyst) reaching out to a CellHawk analyst for assistance on either uploading a file into the system or interpreting the results once an upload is complete.

- Every CellHawk analyst is required to meet Criminal Justice Information Services (CJIS) certification standards in order to work with the application. No vendor analysts have access to the underlying data available in a specific agency's profile with the exemption of exigent support. Two of the CellHawk analysts are designated as certified exigent support staff and have the ability to view data on an agency's profile if the agency grants permission. However, this permission is only granted on a specific basis for work on a specific case and is not granted for the entire agency's available data.

LOCATION

No hardware has been or will be installed to run this specialized mapping software.

Location-based data files are uploaded into CellHawk. Once a file has been uploaded into the system, individual data points are symbolized on a map and subsequent analysis can occur.

UPDATES, UPGRADES, AND CONFIGURATION CHANGES

CellHawk undergoes routine software upgrades as needed to maintain the accuracy and efficiency of this specialized mapping software. No updates, upgrades, or configuration

changes occurred in 2025 that resulted in the expansion or contraction of system access, data retention, or data access.

DEPLOYMENT LOCATION

The surveillance technology was deployed in the following units: Homicide, Special Investigations, Criminal Intelligence, Sex Crimes, Identity Theft, Elder Abuse, Financial Crimes, Gangs, Narcotics, Traffic, and Crime Analysis. These cases could involve all City Council Districts and every SDPD Command.

COMMUNITY COMPLAINTS OR CONCERNS

The Department is committed to protecting civil rights and liberties of our citizens as presented to the City Council prior to approval of this technology. The Department has not received any complaints or concerns about this surveillance technology or received any reports of disproportionate impacts. The Use Policy remains adequate to protect civil rights and civil liberties.

AUDITS OR INVESTIGATIONS

In response to the Privacy Advisory Board's (PAB) Memorandum addressed to San Diego City Council President LaCava and Members of the San Diego City Council on April 17, 2025, which provided a request for more rigorous auditing processes, the SDPD's Research, Analysis, and Planning Division published Department Order (OR) 25-13 on April 25, 2025. This order requires the managing unit (the managing unit is the person(s) recognized as the subject matter expert (SME) for the Transparent and Responsible Use of Surveillance Technology ordinance reporting or who controls the equipment) to prepare for the required Annual Report each year. The OR requires that the SMEs conduct quarterly audits of the equipment they are in charge of, including compiling and tracking information and data listed in SDMC 210.0102(a). On July 15, 2025, an additional Department Order, DO 25-23, was published. This DO requires Department members using any technology or database to enter a reference code/ID or justification for use of the technology or database with either a relevant full eight-digit case number, a full 11-digit event number, or other unique identification code. It requires that users no longer use nonspecific phrases or references and enhances the ability to audit the system.

The audits discovered violations of the Surveillance Use Policy and DO 25-23. The violations include seven (7) instances of users not providing a reference ID in accordance with Department standards. Users and their immediate chain of command were notified of the violation, and corrective instruction was administered on the proper use of reference IDs.

In accordance with OR 25-13, and as an addition to the required quarterly audits by the managing unit, an independent audit was conducted by the Research, Analysis, and Planning Division (RAP)– Inspection and Control Unit. The audits were in addition to the quarterly audits required by the managing unit in OR 25-13. These audits targeted confirmation of the proper use of the technology, as stated in the Use Policy.

This technology was audited on 10 different case numbers, event numbers, or use statistics to verify the proper use of the technology. No unauthorized uses of the technology were located during the audit conducted by RAP.

Any training issues or unintended input errors with this technology were identified and corrected. Continued errors or training issues will result in the user being suspended from the technology until they can be retrained on the technology.

Any substantial non-compliance or intentional misuse will be forwarded to the command or the Internal Affairs Unit for investigation and the subject may have their access permanently removed from the technology.

There was no unauthorized access of this technology and/or no located or reported violations of the Surveillance Use Policy or SDPD Policy or Procedure regarding this technology.

DATA BREACH OR UNAUTHORIZED ACCESS

The City of San Diego's Department of Information Technology and SDPD Information Technology Unit has identified no data breaches or unauthorized access to the data collected by the surveillance technology.

DATA BREACH DETECTION

The City's Department of Information Technology oversees the IT governance process and works with SDPD's Department of IT regarding project execution and risk assessment as well as selecting and approving technology solutions. Cyber security and technology risks are also assessed by the Department of IT. For additional details related to IT governance processes, refer to the information at the following link:

https://www.sandiego.gov/sites/default/files/fy23-fy27-it-strategic-plan-sd.pdf

INFORMATION AND STATISTICS

There are no direct relational crime statistics associated with or produced by the use of this technology.

Should the public want to access crime statistics for the City of San Diego, they can visit the City's *Crime Statistics & Crime Mapping* webpage: Crime Statistics & Crime Mapping | City of San Diego Official Website. The City's neighborhood crime summary dashboard is available at: San Diego Neighborhood Crime Dashboard (arcgis.com). A tab on this dashboard, Crime Data Explorer, allows the user to query crimes specific to a City neighborhood.

Additionally, crime data is also available on the City's Open Data Portal: Datasets - City of San Diego Open Data Portal. This crime data can be downloaded into usable files; also available on this site are dictionaries to help navigate the different data sets.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

The information produced in response to these requests can be viewed on the City of San Diego's CPRA request portal: https://sandiego.nextrequest.com/

REQUEST NUMBER	REQUEST DATE	CLOSED DATE
25-7858	10/07/2025	11/02/2025

ANNUAL COST

CellHawk's cost to the SDPD is approximately $20,780 per fiscal year, and is a recurring cost factored into the Information Technology Unit's budget.

There are no ongoing or personnel costs associated with it.

REQUESTED MODIFICATIONS TO THE USE POLICY

There are no requested modifications to this technology's Use Policy.

San Diego Police Department

CP Clear and TLOxp

Department/Division: Police - Crime Analysis Unit

Related Policy/Procedure:

- DP 1.45 - Use of City/Department Computer Systems
- DP 4.13 - Non-Official or Personal Custody of Records/Files/Recordings Policy

---

DESCRIPTION

CP Clear is an internet-based online service provided by Thomson Reuters. It offers real-time resources to locate information about individuals, utilities, and assets. It is a valuable tool for exigent circumstances such as child abductions, homicides, sex crimes, fugitive apprehension, missing persons, and kidnapping for ransom.

In 2025, approximately 18,800 searches were conducted within the tool.

SHARING OF DATA

Data is queried only by SDPD personnel in the system. There is no data directly input from SDPD into the CP Clear system and the TLOxp system, and therefore, no third-party data sharing exists.

LOCATION

CP Clear and TLOxp are web-based applications. There are no local programs or hardware installed for these technologies on any Department computers.

UPDATES, UPGRADES, AND CONFIGURATION CHANGES

CP Clear and TLOxp undergo routine software upgrades as needed to maintain the accuracy and efficiency of the software. No updates, upgrades, or configuration changes occurred in 2025 that resulted in the expansion or contraction of system access, data retention, or data access.

DEPLOYMENT LOCATION

The surveillance technology was utilized in all SDPD service areas and City Council Districts.

COMMUNITY COMPLAINTS OR CONCERNS

The Department is committed to protecting civil rights and liberties of our citizens as presented to the City Council prior to approval of this technology. The Department has not received any complaints or concerns about this surveillance technology or received any reports of disproportionate impacts. The Use Policy remains adequate to protect civil rights and civil liberties.

AUDITS OR INVESTIGATIONS

In response to the Privacy Advisory Board's (PAB) Memorandum addressed to San Diego City Council President LaCava and Members of the San Diego City Council on April 17, 2025, which provided a request for more rigorous auditing processes, the SDPD's Research,

Analysis, and Planning Division published Department Order (OR) 25-13 on April 25, 2025. This order requires the managing unit (the managing unit is the person(s) recognized as the subject matter expert (SME) for the Transparent and Responsible Use of Surveillance Technology ordinance reporting or who controls the equipment) to prepare for the required Annual Report each year. The OR requires that the SMEs conduct quarterly audits of the equipment they are in charge of, including compiling and tracking information and data listed in SDMC 210.0102(a). On July 15, 2025, an additional Department Order, DO 25-23, was published. This DO requires Department members using any technology or database to enter a reference code/ID or justification for use of the technology or database with either a relevant full eight-digit case number, a full 11-digit event number, or other unique identification code. It requires that users no longer use nonspecific phrases or references and enhances the ability to audit the system.

The quarterly audits of the CP Clear system discovered violations of the Surveillance Use Policy and DO 25-23. The violations include 22 of the 40 sampled users not providing a reference ID in accordance with Department standards, totaling 1,191 searches. Users and their immediate chain of command were notified of the violation, and corrective instruction was administered on the proper use of reference IDs.

The quarterly audits of the TLOxp system discovered violations of the Surveillance Use Policy and DO 25-23. The violations include 22 of the 40 sampled users not providing a reference ID in accordance with Department standards, totaling 2,112 searches. Users and their immediate chain of command were notified of the violation, and corrective instruction was administered on the proper use of reference IDs.

In accordance with OR 25-13, and as an addition to the required quarterly audits by the managing unit, an independent audit was conducted by the Research, Analysis, and Planning Division (RAP)– Inspection and Control Unit. The audits were in addition to the quarterly audits required by the managing unit in OR 25-13. These audits targeted confirmation of the proper use of the technology, as stated in the Use Policy.

The CP Clear system was audited on 20 different case numbers, event numbers, or use statistics to verify the proper use of the technology. No unauthorized uses of the technology were located during the audit conducted by RAP.

The TLOxp system was audited on 40 different case numbers, event numbers, or use statistics to verify the proper use of the technology. No unauthorized uses of the technology were located during the audit conducted by RAP.

Any training issues or unintended input errors with this technology were identified and corrected. Continued errors or training issues will result in the user being suspended from the technology until they can be retrained on the technology.

Any substantial non-compliance or intentional misuse will be forwarded to the command or the Internal Affairs Unit for investigation and the subject may have their access permanently removed from the technology.

There was no unauthorized access of this technology and/or no located or reported violations of the Surveillance Use Policy or SDPD Policy or Procedure regarding this technology.

To further assist with auditing and compliance with the Use Policy, reference ID characters became required for both technologies in 2025.

DATA BREACH OR UNAUTHORIZED ACCESS

The City of San Diego's Department of Information Technology and SDPD Information Technology Unit has identified no data breaches or unauthorized access to the data collected by the surveillance technology.

DATA BREACH DETECTION

The City's Department of Information Technology oversees the IT governance process and works with SDPD's Department of IT regarding project execution and risk assessment as well as selecting and approving technology solutions. Cyber security and technology risks are also assessed by the Department of IT. For additional details related to IT governance processes, refer to the information at the following link:

https://www.sandiego.gov/sites/default/files/fy23-fy27-it-strategic-plan-sd.pdf

INFORMATION AND STATISTICS

There are no direct relational crime statistics associated with or produced by the use of this technology.

Should the public want to access crime statistics for the City of San Diego, they can visit the City's *Crime Statistics & Crime Mapping* webpage: Crime Statistics & Crime Mapping | City of San Diego Official Website. The City's neighborhood crime summary dashboard is available at: San Diego Neighborhood Crime Dashboard (arcgis.com). A tab on this dashboard, Crime Data Explorer, allows the user to query crimes specific to a City neighborhood.

Additionally, crime data is also available on the City's Open Data Portal: Datasets - City of San Diego Open Data Portal. This crime data can be downloaded into usable files; also available on this site are dictionaries to help navigate the different data sets.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

The information produced in response to these requests can be viewed on the City of San Diego's CPRA request portal: https://sandiego.nextrequest.com/

REQUEST NUMBER	REQUEST DATE	CLOSED DATE
25-7858**	10/07/2025	11/02/2025
25-10375**	12/26/2025	Open
25-9793**	12/08/2025	12/31/2025

*Applies to both technologies.

ANNUAL COST

CP Clear's cost to SDPD is approximately $24,000 per fiscal year and is a recurring cost factored into the Information Technology Unit's budget.

There are no ongoing or personnel costs associated with the tool.

TLOxp's cost to SDPD is approximately $15,000 per fiscal year and is a recurring cost factored into the Information Technology Unit's budget.

There are no ongoing or personnel costs associated with the tool.

REQUESTED MODIFICATIONS TO THE USE POLICY

There are no requested modifications to these technologies' Use Policies.

San Diego Police Department

Nighthawk (Data Analytics Tool)

Department/Division: Police - Investigations II - Robbery

Related Policy/Procedure:

- DP 1.45 – Use of City or Department Computer Systems

DESCRIPTION

The San Diego Police Department utilizes the Leads-Online Nighthawk system to assist investigators with data analysis. The system provides a comprehensive data analysis tool for investigators and department analysts. Nighthawk allows its users to integrate collected data from various sources. The system organizes and provides the user an efficient means of searching through large amounts of collected data during a criminal investigation.

The San Diego Police Department currently has 40 registered accounts. In 2025, the Nighthawk system was accessed 2,732 times by its registered users.

SHARING OF DATA

Data is not acquired through the use of Nighthawk, as it is merely a data analysis tool used to integrate collected data from different sources.

Uploaded files can be viewed by either Detectives or Crime Analysts that upload files into the system, sometimes working in conjunction with one another on an investigation.

Additionally, files retained in the system can be accessed by Nighthawk analysts. Typically, the scenario in which this would happen involves the user (Detective or Crime Analyst) reaching out to a Nighthawk analyst for assistance on either uploading a file into the system or interpreting the results once an upload is complete.

Every investigator or analyst assigned a Nighthawk license is required to meet Criminal Justice Information Services (CJIS) certification standards in order to work with the application. The Nighthawk licenses that provide access to the system are assigned to an individual investigator or analyst.

LOCATION

Nighthawk is a cloud-based application used by investigators and analysts. Investigators and analysts assigned to investigative units that frequently handle cases that require extensive data analysis are provided access to the Nighthawk system.

UPDATES, UPGRADES, AND CONFIGURATION CHANGES

There have been no updates, upgrades, or configuration changes in 2025.

DEPLOYMENT LOCATION

This surveillance technology is a cloud-based application for integrating data from various sources. It was utilized during investigations from all service areas within the City of San Diego.

COMMUNITY COMPLAINTS OR CONCERNS

The Department is committed to protecting civil rights and liberties of all citizens as presented to the City Council prior to the approval of this technology. The Department did not receive any complaints or concerns regarding this surveillance technology or receive any reports of disproportionate impacts. The Use Policy protected civil rights and liberties.

AUDITS OR INVESTIGATIONS

In response to the Privacy Advisory Board's (PAB) Memorandum addressed to San Diego City Council President LaCava and Members of the San Diego City Council on April 17, 2025, which provided a request for more rigorous auditing processes, the SDPD's Research, Analysis, and Planning Division published Department Order (OR) 25-13 on April 25, 2025. This order requires the managing unit (the managing unit is the person(s) recognized as the subject matter expert (SME) for the Transparent and Responsible Use of Surveillance Technology ordinance reporting or who controls the equipment) to prepare for the required Annual Report each year. The OR requires that the SMEs conduct quarterly audits of the equipment they are in charge of, including compiling and tracking information and data listed in SDMC 210.0102(a). On July 15, 2025, an additional Department Order, DO 25-23, was published. This DO requires Department members using any technology or database to enter a reference code/ID or justification for use of the technology or database with either a relevant full eight-digit case number, a full 11-digit event number, or other unique identification code. It requires that users no longer use nonspecific phrases or references and enhances the ability to audit the system.

In accordance with OR 25-13, and as an addition to the required quarterly audits by the managing unit, an independent audit was conducted by the Research, Analysis, and Planning Division (RAP)– Inspection and Control Unit. The audits were in addition to the quarterly audits required by the managing unit in OR 25-13. These audits targeted confirmation of the proper use of the technology, as stated in the Use Policy.

The Nighthawk application is consistently audited throughout the year. The registered users are changed periodically based on their assignment and amount of application use. This technology requires legal approval before utilizing the system. The audits were procedural. No unauthorized uses of the technology were located during the audit conducted by RAP.

Any substantial non-compliance or intentional misuse will be forwarded to the command or the Internal Affairs Unit for investigation and the subject may have their access permanently removed from the technology.

There was no unauthorized access of this technology and/or no located or reported violations of the Surveillance Use Policy or SDPD Policy or Procedure regarding this technology.

DATA BREACH OR UNAUTHORIZED ACCESS

The City of San Diego's Department of Information Technology and SDPD Information Technology Unit has identified no data breaches or unauthorized access to the data collected by the surveillance technology.

DATA BREACH DETECTION

The City's Department of Information Technology oversees the IT governance process and works with SDPD's Department of IT regarding project execution and risk assessment as well as selecting and approving technology solutions. Cyber security and technology risks are also assessed by the Department of IT. For additional details related to IT governance processes, refer to the information at the following link:

https://www.sandiego.gov/sites/default/files/fy23-fy27-it-strategic-plan-sd.pdf

INFORMATION AND STATISTICS

There are no direct relational crime statistics associated with or produced by the use of this technology.

Should the public want to access crime statistics for the City of San Diego, they can visit the City's *Crime Statistics & Crime Mapping* webpage: Crime Statistics & Crime Mapping | City of San Diego Official Website. The City's neighborhood crime summary dashboard is available at: San Diego Neighborhood Crime Dashboard (arcgis.com). A tab on this dashboard, Crime Data Explorer, allows the user to query crimes specific to a City neighborhood.

Additionally, crime data is also available on the City's Open Data Portal: Datasets - City of San Diego Open Data Portal. This crime data can be downloaded into usable files; also available on this site are dictionaries to help navigate the different data sets.

In 2025, the Nighthawk system was accessed 2,732 times by its registered users. The application was utilized in a multitude of criminal investigations.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

The information produced in response to these requests can be viewed on the City of San Diego's CPRA request portal: https://sandiego.nextrequest.com/

REQUEST NUMBER	REQUEST DATE	CLOSED DATE
25-7858	10/07/2025	11/02/2025

ANNUAL COST

The cost for the service is $87,960 a year. This amount is the cost of the service for FY2026 as part of a five-year contract with Leads-Online. It provides Nighthawk licenses and access for 40 department members.

The funding source for the Nighthawk system is the Department of Justice (DOJ) seized assets fund.

REQUESTED MODIFICATIONS TO THE USE POLICY

There have been no requested modifications to this technology Use Policy.

San Diego Police Department

RealQuest Online Services

Department/Division: Police - Traffic

Related Policy/Procedure:

- DP 1.45 – Use of City / Department Computer Systems

DESCRIPTION

The San Diego Police Department's Abandoned Vehicle Abatement Unit utilizes Realquest Online Services to address complaints made by community members regarding abandoned or inoperable vehicles stored on private property using public records and open-source information.

In 2025, RealQuest Online Services were utilized approximately nine (9) times for the purpose of obtaining contact information of a property owner. The property owner was then contacted in relation to a community member's complaint regarding an abandoned or inoperable vehicle stored on their property.

SHARING OF DATA

The information obtained from RealQuest Online Services is attached to an abatement civil case and is filed with City staff. SDPD does not share data gathered with any other entities.

LOCATION

RealQuest Online Services is an online/internet-based platform and is only accessed through secure Department computers via user login authentication. The data accessed is not stored on City hardware unless downloaded from the web application for use in a qualifying investigation. The downloaded data would then be maintained in an active case file.

UPDATES, UPGRADES, AND CONFIGURATION CHANGES

There have been no updates, upgrades, or configuration.

DEPLOYMENT LOCATION

This surveillance technology was deployed by the Abandoned Vehicle Abatement Unit for all police service areas.

COMMUNITY COMPLAINTS OR CONCERNS

The SDPD is committed to protecting civil rights and liberties of our citizens as presented to the City Council prior to approval of this technology. The SDPD has not received any complaints or concerns about this surveillance technology or received any reports of disproportionate impacts. The Use Policy continues to protect civil rights and civil liberties.

AUDITS OR INVESTIGATIONS

In response to the Privacy Advisory Board's (PAB) Memorandum addressed to San Diego City Council President LaCava and Members of the San Diego City Council on April 17, 2025,

which provided a request for more rigorous auditing processes, the SDPD's Research, Analysis, and Planning Division published Department Order (OR) 25-13 on April 25, 2025. This order requires the managing unit (the managing unit is the person(s) recognized as the subject matter expert (SME) for the Transparent and Responsible Use of Surveillance Technology ordinance reporting or who controls the equipment) to prepare for the required Annual Report each year. The OR requires that the SMEs conduct quarterly audits of the equipment they are in charge of, including compiling and tracking information and data listed in SDMC 210.0102(a). On July 15, 2025, an additional Department Order, DO 25-23, was published. This DO requires Department members using any technology or database to enter a reference code/ID or justification for use of the technology or database with either a relevant full eight-digit case number, a full 11-digit event number, or other unique identification code. It requires that users no longer use nonspecific phrases or references and enhances the ability to audit the system.

In accordance with OR 25-13, and as an addition to the required quarterly audits by the managing unit, an independent audit was conducted by the Research, Analysis, and Planning Division (RAP)– Inspection and Control Unit. The audits were in addition to the quarterly audits required by the managing unit in OR 25-13. These audits targeted confirmation of the proper use of the technology, as stated in the Use Policy.

This technology was audited on 5 different case numbers, event numbers, or use statistics to verify the proper use of the technology. No unauthorized uses of the technology were located during the audit conducted by RAP.

Any substantial non-compliance or intentional misuse will be forwarded to the command or the Internal Affairs Unit for investigation and the subject may have their access permanently removed from the technology.

There was no unauthorized access of this technology and/or no located or reported violations of the Surveillance Use Policy or SDPD Policy or Procedure regarding this technology.

DATA BREACH OR UNAUTHORIZED ACCESS

The City of San Diego's Department of Information Technology and SDPD Information Technology Unit has identified no data breaches or unauthorized access to the data collected by the surveillance technology.

DATA BREACH DETECTION

The City's Department of Information Technology oversees the IT governance process and works with SDPD's Department of IT regarding project execution and risk assessment as well as selecting and approving technology solutions. Cyber security and technology risks are also assessed by the Department of IT. For additional details related to IT governance processes, refer to the information at the following link:

https://www.sandiego.gov/sites/default/files/fy23-fy27-it-strategic-plan-sd.pdf

INFORMATION AND STATISTICS

There are no direct relational crime statistics associated with or produced by the use of this technology.

Should the public want to access crime statistics for the City of San Diego, they can visit the City's *Crime Statistics & Crime Mapping* webpage: Crime Statistics & Crime Mapping | City of

San Diego Official Website. The City's neighborhood crime summary dashboard is available at: San Diego Neighborhood Crime Dashboard (arcgis.com). A tab on this dashboard, Crime Data Explorer, allows the user to query crimes specific to a City neighborhood.

Additionally, crime data is also available on the City's Open Data Portal: Datasets - City of San Diego Open Data Portal. This crime data can be downloaded into usable files; also available on this site are dictionaries to help navigate the different data sets.

Realquest Online Services was utilized nine times for the purpose of obtaining contact information of a property owner. Of the nine completed cases, the Abandoned Vehicle Abatement Unit was successful in gaining compliance from all property owners. The vehicles were moved, and further proceedings were avoided.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

The information produced in response to these requests can be viewed on the City of San Diego's CPRA request portal: https://sandiego.nextrequest.com/

REQUEST NUMBER	REQUEST DATE	CLOSED DATE
25-7858	10/07/2025	11/02/2025

ANNUAL COST

The Realquest Online Services annual subscription costs approximately $2,496.36, including a 3% yearly increase and is funded through the Department's General Fund.

REQUESTED MODIFICATIONS TO THE USE POLICY

There are no requested modifications.

San Diego Police Department

Vigilant: Automated License Plate Recognition (ALPR)

Department/Division: Police - Real Time Operations Center

Related Policy/Procedure:

- DP 1.51 Automatic License Plate Recognition (ALPR)
- DP 3.02 Property and Evidence

DESCRIPTION

Vigilant ALPR utilizes mobile and fixed cameras to scan license plates and compare the license plates against a database of wanted vehicles. This data is also queried by officers and investigators during investigations to identify suspect vehicles in real time or during follow-up investigations.

The San Diego Police Department subscribes to Vigilant in order to gain access to their nationwide database. The SDPD does not have any hardware assets and therefore does not contribute data to the Vigilant system.

SHARING OF DATA

The San Diego Police Department does not gather information or data. Vigilant technology is a web-based system that collects data from legally obtained sources and shares it with authorized users.

The legally obtained resources are from California law enforcement agencies and private companies (Towing Companies) which collect data using ALPR. Each individual agency or company then shares the data with Vigilant.

LOCATION

Vigilant is a web-based system and SDPD does not have any physical equipment.

UPDATES, UPGRADES, AND CONFIGURATION CHANGES

No updates, upgrades, or configurations were done to the system that resulted in the expansion or contraction of system access, data retention, or data access.

DEPLOYMENT LOCATION

Vigilant is a web-based system and SDPD does not have any physical equipment.

COMMUNITY COMPLAINTS OR CONCERNS

The Department is committed to protecting civil rights and liberties of our citizens as presented to the City Council prior to approval of this technology. The Department has not received any complaints or concerns about this surveillance technology or received any reports of disproportionate impacts. The Use Policy continues to protect civil rights and civil liberties.

AUDITS OR INVESTIGATIONS

In response to the Privacy Advisory Board's (PAB) Memorandum addressed to San Diego City Council President LaCava and Members of the San Diego City Council on April 17, 2025, which provided a request for more rigorous auditing processes, the SDPD's Research, Analysis, and Planning Division published Department Order (OR) 25-13 on April 25, 2025. This order requires the managing unit (the managing unit is the person(s) recognized as the subject matter expert (SME) for the Transparent and Responsible Use of Surveillance Technology ordinance reporting or who controls the equipment) to prepare for the required Annual Report each year. The OR requires that the SMEs conduct quarterly audits of the equipment they are in charge of, including compiling and tracking information and data listed in SDMC 210.0102(a). On July 15, 2025, an additional Department Order, DO 25-23, was published. This DO requires Department members using any technology or database to enter a reference code/ID or justification for use of the technology or database with either a relevant full eight-digit case number, a full 11-digit event number, or other unique identification code. It requires that users no longer use nonspecific phrases or references and enhances the ability to audit the system.

In accordance with OR 25-13, and as an addition to the required quarterly audits by the managing unit, an independent audit was conducted by the Research, Analysis, and Planning Division (RAP)– Inspection and Control Unit. The audits were in addition to the quarterly audits required by the managing unit in OR 25-13. These audits targeted confirmation of the proper use of the technology, as stated in the Use Policy.

This technology was audited on 40 different case numbers, event numbers, or use statistics to verify the proper use of the technology. No unauthorized uses of the technology were located during the audit conducted by RAP.

Any substantial non-compliance or intentional misuse will be forwarded to the command or the Internal Affairs Unit for investigation and the subject may have their access permanently removed from the technology.

There was no unauthorized access of this technology and/or no located or reported violations of the Surveillance Use Policy or SDPD Policy or Procedure regarding this technology.

DATA BREACH OR UNAUTHORIZED ACCESS

The City of San Diego's Department of Information Technology and SDPD Information Technology Unit has identified no data breaches or unauthorized access to the data collected by the surveillance technology.

DATA BREACH DETECTION

The City's Department of Information Technology oversees the IT governance process and works with SDPD's Department of IT regarding project execution and risk assessment as well as selecting and approving technology solutions. Cyber security and technology risks are also assessed by the Department of IT. For additional details related to IT governance processes, refer to the information at the following link:

https://www.sandiego.gov/sites/default/files/fy23-fy27-it-strategic-plan-sd.pdf

Encryption, firewalls, authentication, and other reasonable security measures shall be utilized to protect digital evidence from the Vigilant ALPR database.

INFORMATION AND STATISTICS

There are no direct relational crime statistics associated with or produced by the use of this technology.

Should the public want to access crime statistics for the City of San Diego, they can visit the City's *Crime Statistics & Crime Mapping* webpage: Crime Statistics & Crime Mapping | City of San Diego Official Website. The City's neighborhood crime summary dashboard is available at: San Diego Neighborhood Crime Dashboard (arcgis.com). A tab on this dashboard, Crime Data Explorer, allows the user to query crimes specific to a City neighborhood.

Additionally, crime data is also available on the City's Open Data Portal: Datasets - City of San Diego Open Data Portal. This crime data can be downloaded into usable files; also available on this site are dictionaries to help navigate the different data sets.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

The information produced in response to these requests can be viewed on the City of San Diego's CPRA request portal: https://sandiego.nextrequest.com/

REQUEST NUMBER	REQUEST DATE	CLOSED DATE
25-7858	10/07/2025	11/02/2025
25-6782	09/01/2025	09/26/2025
25-6692	08/28/2025	11/06/2025

ANNUAL COST

In2025 the cost of access to the commercial version of Vigilant was $54,750.

All funding sources were from the City's General Fund and will continue in 2027.

REQUESTED MODIFICATIONS TO THE USE POLICY

No modifications were requested for this use policy.

San Diego Police Department
Overt Technologies

SDPD
ONE TEAM. ONE MISSION.

San Diego Police Department

ARTECO – Camera Trailer - Skywatch

Department/Division: Police - Operational Support - Logistics Unit

Related Policy/Procedure:

- DP 3.02 – Impound, Release, and Disposal of Property, Evidence and Articles Missing Identification Marks
- DP 1.49 – AXON Body Worn Cameras

DESCRIPTION

These three technologies are assigned to the Department's Logistics Unit and provide support for first responders and command personnel during critical incidents, disasters, special events, large gatherings, as well as all hazard events. They are as follows:

The Skywatch and Terrahawk Observation Towers provide a raised platform for viewing by up to two personnel. These units are equipped with one pan tilt zoom (PTZ) cameras and can provide real-time video to the person occupying Skywatch & Terrahawk during an incident. The Skywatch & Terrahawk Towers are used for live situational awareness, enhanced security overwatch during large events and gatherings and as a visual deterrent. In 2025, this technology was used during eight events.

Command Vehicles utilize the ARTECO video management system (VMS)/camera to provide a camera and viewing platform to view real-time video around a command post. The real-time video provides situational awareness and security to personnel and decision-makers working at a command post. This surveillance technology is mounted onboard three command vehicles (Mobile 1, 4 & 7). The surveillance technology was used for live situational awareness, enhanced security overwatch during large events and gatherings and as a visual deterrent. in 2025, this technology was deployed during 20 events.

The Camera Trailer Camera Systems are used to support first responders and command personnel during critical incidents, disasters, special events, and large gatherings by providing video to a command post from a remote location. The cameras have the ability to provide real-time video in order to furnish critical information to decision makers, as well as record video to retain potential evidence. The Camera Trailer Camera Systems' six mobile trailers are used for live situational awareness, enhanced security overwatch during large events and gatherings, as well as being used as a visual deterrent. In 2025 , this technology was deployed during 17 events.

SHARING OF DATA

The Logistical Support Unit received no data-sharing requests from these surveillance technologies during the 2025 calendar year.

LOCATION

These technologies are mounted onboard the specific conveyances listed above.

UPDATES, UPGRADES, AND CONFIGURATION CHANGES

There have been no updates, upgrades, or configuration changes that expanded or reduced the surveillance technology capabilities of these items.

DEPLOYMENT LOCATION

Equipment Type	Deployment Area	Reason for Deployment
Command Vehicle (ARTECO)	Northern Division	Special Event Operations
Command Vehicle (ARTECO)	Central Division	Special Event Operations
Command Vehicle (ARTECO)	Central Division	Special Event Operations
Command Vehicle (ARTECO)	Southeastern Division	Special Event Operations
Command Vehicle (ARTECO)	Northern Division	Special Event Operations
Command Vehicle (ARTECO)	Central Division	Special Event Operations
Command Vehicle (ARTECO)	Western Division	Special Event Operations
Command Vehicle (ARTECO)	Northeastern Division	Missing Person
Command Vehicle (ARTECO)	Northwestern Division	Special Event Operations
Command Vehicle (ARTECO)	Northern Division	Homicide
Command Vehicle (ARTECO)	Western Division	Special Event Operations
Command Vehicle (ARTECO)	Central Division	Special Event Operations
Command Vehicle (ARTECO)	Western Division	Special Event Operations
Command Vehicle (ARTECO)	Western Division	Special Event Operations
Command Vehicle (ARTECO)	Northern Division	Special Event Operations
Command Vehicle (ARTECO)	Northwestern Division	Special Event Operations
Command Vehicle (ARTECO)	Northern Division	Homicide
Command Vehicle (ARTECO)	Central Division	Special Event Operations
Command Vehicle (ARTECO)	Central Division	Special Event Operations
Command Vehicle (ARTECO)	Northern Division	Special Event Operations
Camera Trailers	Central Division	Special Event Operations
Camera Trailers	Central Division	Special Event Operations
Camera Trailers	Central Division	Special Event Operations
Camera Trailers	Central Division	Special Event Operations
Camera Trailers	Central Division	Special Event Operations
Camera Trailers	Western Division	Special Event Operations
Camera Trailers	Central Division	Special Event Operations
Camera Trailers	Western Division	Special Event Operations
Camera Trailers	Western Division	Special Event Operations
Camera Trailers	Central Division	Investigations Detail
Camera Trailers	Central Division	Special Event Operations

Equipment Type (continued)	Deployment Area	Reason for Deployment
Camera Trailers	Central Division	Special Event Operations
Camera Trailers	Harbor Police Department	Special Event Operations
Camera Trailers	Central Division	Special Event Operations
Camera Trailers	Northern Division	Special Event Operations
Camera Trailers	Northern Division	Special Event Operations
Camera Trailers	Northeastern Division	Special Event Operations
SKYWATCH Observation Tower	Western Division	Special Event Operations
SKYWATCH Observation Tower	Central Division	Special Event Operations
SKYWATCH Observation Tower	Central Division	Special Event Operations
TERRAHAWK Observation Tower	Central Division	Special Event Operations
TERRAHAWK Observation Tower	Western Division	Special Event Operations
TERRAHAWK Observation Tower	Central Division	Special Event Operations
TERRAHAWK Observation Tower	Central Division	Special Event Operations
TERRAHAWK Observation Tower	Central Division	Special Event Operations

COMMUNITY COMPLAINTS OR CONCERNS

The Department is committed to protecting civil rights and liberties of our citizens as presented to the City Council prior to approval of this technology. The Department has not received any complaints or concerns about this surveillance technology or received any reports of disproportionate impacts. The Use Policies continue to protect civil rights and civil liberties.

AUDITS OR INVESTIGATIONS

In response to the Privacy Advisory Board's (PAB) Memorandum addressed to San Diego City Council President LaCava and Members of the San Diego City Council on April 17, 2025, which provided a request for more rigorous auditing processes, the SDPD's Research, Analysis, and Planning Division published Department Order (OR) 25-13 on April 25, 2025. This order requires the managing unit (the managing unit is the person(s) recognized as the subject matter expert (SME) for the Transparent and Responsible Use of Surveillance Technology ordinance reporting or who controls the equipment) to prepare for the required Annual Report each year. The OR requires that the SMEs conduct quarterly audits of the equipment they are in charge of, including compiling and tracking information and data listed in SDMC 210.0102(a). On July 15, 2025, an additional Department Order, DO 25-23, was published. This DO requires Department members using any technology or database to enter a reference code/ID or justification for use of the technology or database with either a relevant full eight-digit case number, a full 11-digit event number, or other unique identification code. It requires that users no longer use nonspecific phrases or references and enhances the ability to audit the system.

In accordance with OR 25-13, and as an addition to the required quarterly audits by the managing unit, an independent audit was conducted by the Research, Analysis, and Planning Division (RAP)– Inspection and Control Unit. The audits were in addition to the quarterly

audits required by the managing unit in OR 25-13. These audits targeted confirmation of the proper use of the technology, as stated in the Use Policy.

The Camera Trailer Camera System was audited on 17 different case numbers, event numbers, or use statistics to verify the proper use of the technology. No unauthorized uses of the technology were located during the audit conducted by RAP.

The Arteco technology was audited on 25 different case numbers, event numbers, or use statistics to verify the proper use of the technology. No unauthorized uses of the technology were located during the audit conducted by RAP.

The Skywatch and Terrahawk technologies were audited on 3 different case numbers, event numbers, or use statistics to verify the proper use of the technology. No unauthorized uses of the technology were located during the audit conducted by RAP.

Any substantial non-compliance or intentional misuse will be forwarded to the command or the Internal Affairs Unit for investigation and the subject may have their access permanently removed from the technology.

There was no unauthorized access of this technology and/or no located or reported violations of the Surveillance Use Policy or SDPD Policy or Procedure regarding this technology.

DATA BREACH OR UNAUTHORIZED ACCESS

The City of San Diego's Department of Information Technology and SDPD Information Technology Unit has identified no data breaches or unauthorized access to the data collected by the surveillance technology.

DATA BREACH DETECTION

The City's Department of Information Technology oversees the IT governance process and works with SDPD's Department of IT regarding project execution and risk assessment as well as selecting and approving technology solutions. Cyber security and technology risks are also assessed by the Department of IT. For additional details related to IT governance processes, refer to the information at the following link:

https://www.sandiego.gov/sites/default/files/fy23-fy27-it-strategic-plan-sd.pdf

INFORMATION AND STATISTICS

There are no direct relational crime statistics associated with or produced by the use of this technology.

Should the public want to access crime statistics for the City of San Diego, they can visit the City's *Crime Statistics & Crime Mapping* webpage: Crime Statistics & Crime Mapping | City of San Diego Official Website. The City's neighborhood crime summary dashboard is available at: San Diego Neighborhood Crime Dashboard (arcgis.com). A tab on this dashboard, Crime Data Explorer, allows the user to query crimes specific to a City neighborhood.

Additionally, crime data is also available on the City's Open Data Portal: Datasets - City of San Diego Open Data Portal. This crime data can be downloaded into usable files; also available on this site are dictionaries to help navigate the different data sets.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

The information produced in response to these requests can be viewed on the City of San Diego's CPRA request portal: https://sandiego.nextrequest.com/

REQUEST NUMBER	REQUEST DATE	CLOSED DATE
25-7858	10/07/2025	11/02/2025

ANNUAL COST

$25,000.00 annual software & up-date PO through "Aggerate Way"

$25,000.00 annual maintenance PO for through "DVR Simple Solutions"

$25,000.00 annual parts PO through "Willy's Electronic Supply" (This is a shared PO which is also used for security card access reader parts)

All three PO's use City General Funds.

REQUESTED MODIFICATIONS TO THE USE POLICY

There are no requested modifications to these technologies' Use Policies.

San Diego Police Department

Automated License Plate Recognition (ALPR)

Department/Division: Police - Real Time Operations Center

Related Policy/Procedure:

- DP 1.51 Automatic License Plate Recognition (ALPR)
- DP 3.02 Property and Evidence

DESCRIPTION

210.0102(a)(1) A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the surveillance technology.

Automated License Plate Recognition (ALPR) is a camera-based system that captures images of rear license plates on vehicles traveling or parked in public areas. SDPD uses vendor-provided Flock cameras installed on streetlights at approximately 500 locations citywide. The system automatically reads the plate number and records the date, time, and location of the scan, and may also capture basic vehicle descriptors such as make, model, and color. The information is encrypted and transmitted to a secure database that can only be accessed by authorized SDPD personnel. ALPR data is retained for up to 30 days and is automatically deleted unless it is preserved as evidence in an active investigation.

ALPR may only be used for official law enforcement purposes, such as locating vehicles connected to investigations, supporting critical incident response, and helping locate at-risk missing persons. Its use is governed by the ALPR Use Policy, which prohibits misuse, including using the system to invade privacy, discriminate, or for any personal or non-law enforcement purpose. Access is restricted to trained personnel, and users must complete ALPR-specific training on lawful use, privacy, and data handling before receiving access. Compliance is reinforced through audits, access controls, and disciplinary review for violations.

In 2025:

- Officers conducted more than 244,000 investigative searches of ALPR data, which played a key role in advancing 361 cases.
- The technology supported the arrest of 269 suspects and the recovery of 12 firearms and approximately $3.1 million in stolen property, including 259 stolen vehicles.
- Of the 28 homicides San Diego experienced in 2025, ALPR technology aided in nearly a third of them.
- ALPR also helped locate four missing persons.

Beyond arrests, ALPR improves precision policing, helping officers rely on verified information rather than broad patrols. This reduces unnecessary community contacts, conserves resources, and increases safety for both officers and residents.

SHARING OF DATA

210.0102(a)(2) Whether and how often data acquired through the use of the surveillance technology was shared with any non-City entities, the name of any recipient entity, the types of data disclosed,

under what legal standards the information was disclosed, and the justification for the disclosure, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the City.

In addition to providing ALPR data to the District Attorney's/City Attorney's Office for criminal prosecution, SDPD shared ALPR images or data with other California law enforcement agencies when there was a legitimate investigative need and after a qualifying reason had occurred, such as a homicide, shooting, or public safety emergency. In 2025, SDPD shared with 36 such entities. This sharing is authorized under SB 34.

Each request SDPD receives from a non-City entity is required to be evaluated to ensure it is a proper search that complies with California law, including SB 54, and the Department's Use Policy. SDPD's policy requires that ALPR searches be for a legitimate law enforcement purpose and prohibits improper uses, such as invading privacy where a reasonable expectation of privacy exists; using ALPR in a discriminatory manner or to target protected characteristics; harassment or intimidation; or violating constitutional rights.

To aid in this evaluation and ensure accountability, SDPD requires requesting agencies to provide a case number tied to the investigation, which is logged in the ALPR system. Additionally, beginning in December 2025, all officers were prompted to select the kind of case that's being investigated from a drop-down menu in the Flock system.

In May 2025, after receiving guidance from the California Department of Justice, SDPD ended all data sharing with federal and out-of-state agencies. This decision was formalized in Department Order #25-19. Before this order was issued, the Department shared ALPR data and/or images with eight federal and out-of-state agencies in response to several serious crimes, such as human trafficking, an assault against an officer, and crimes against children. None of these cases were related to immigration enforcement.

After the Department issued the order ending such sharing, there was one instance in which ALPR information was shared with an out-of-state agency to assist in a domestic violence-related incident. This search was immediately flagged, and the officer was contacted by a supervisor. The officer received additional training.

See Addendum A for a comprehensive list of outside agency data sharing.

LOCATION

210.0102(a)(3) A description of the physical objects to which the surveillance technology hardware was installed, if applicable, and without revealing the specific location of the hardware, and a breakdown of the data sources applied or related to the surveillance technology software.

The Smart Streetlights System, which includes situational cameras and ALPR cameras, is attached to City of San Diego streetlight poles. The locations of Smart Streetlights are publicly available on the city's website.

UPDATES, UPGRADES, AND CONFIGURATION CHANGES

210.0102(a)(4) A list of the software updates, hardware upgrades, and system configuration changes that expanded or reduced the surveillance technology capabilities, as well as a description of the

reason for the changes, except that no confidential or sensitive information should be disclosed that would violate any applicable law or undermine the legitimate security interests of the City.

In December 2025, the Flock operating system was updated to include a more robust audit log. This update included the addition of anonymized user identification, which created unique user identification numbers for officers, and an Offense Type drop-down menu. The Offense Type drop-down menu allows officers to select the type of case or investigation associated with each search, improving documentation and accountability for system use.

DEPLOYMENT LOCATION

210.0102(a)(5) A description of where the surveillance technology was deployed geographically, by each City Council District or police area, in the applicable year.

ALPR cameras are present in all council districts and police divisions. Current camera locations can be reviewed at the following link:

https://webmaps.sandiego.gov/portal/apps/webappviewer/index.html

COMMUNITY COMPLAINTS OR CONCERNS

210.0102(a)(6) A summary of any community complaints or concerns about the surveillance technology and an analysis of its Surveillance Use Policy, including whether it is adequate in protecting civil rights and civil liberties, and whether, and to what extent, the use of the surveillance technology disproportionately impacts certain groups or individuals.

Community complaints and concerns over the Department's ALPR program have touched on privacy, data sharing, transparency, retention, accuracy, auditing, cybersecurity, and the potential for disproportionate impacts. SDPD has revised its policy, increased oversight, and expanded public reporting in an effort to address these concerns.

Data sharing with federal agencies: Community members fear ALPR data could be shared with federal agencies for immigration purposes. In May 2025, after guidance from the California Department of Justice, SDPD ended all ALPR data sharing with federal and out-of-state agencies. This restriction was reiterated in SDPD policy following revisions shaped by community input and recommendations from the Privacy Advisory Board. SDPD has never shared ALPR information for immigration-related purposes.

Auditing practices: Some community members have raised concerns that ALPR use is not audited frequently enough or made transparent to the public. Beginning in 2025, SDPD implemented weekly audits to ensure compliance with state laws like SB 34, the TRUST Ordinance, and SDPD's Use Policy. SDPD also worked with its vendor to require officers to select an offense type from a drop-down menu in the Flock system for each search. These selections will soon be reflected in publicly available audit reports posted to the City's website.

Retention and tracking: Some community members have concerns that the 30-day retention period is too long, and that ALPR primarily collects information on law-abiding drivers. SDPD's 30-day retention period is shorter than many large cities and other jurisdictions in San Diego County. SDPD believes 30 days is the minimum retention period that maintains investigative effectiveness while balancing privacy. Most ALPR data is automatically purged

without ever being viewed, and only authorized SDPD personnel may access the system for legitimate law enforcement purposes.

System accuracy: Community members have brought up the potential for plate misreads that may unintentionally impact uninvolved individuals. SDPD requires officers to confirm ALPR information before taking action by (1) visually confirming the plate and state of origin, and (2) confirming the alert status through the National Crime Information Center (NCIC) database.

Cybersecurity and vendor constraints: Some community members have expressed concern that the system could be hacked or that the vendor could share data with the federal government. Flock Safety follows strict cybersecurity protocols, undergoes regular third-party audits, uses encryption and role-based access controls, operates on AWS, and is CJIS compliant. Sharing ALPR data with federal agencies is prohibited by SDPD policy, and contractors and subcontractors are required to comply with that policy. Violations could result in contract termination.

Civil rights protections: Some community members worry the system could be used to violate people's civil rights. SDPD's Use Policy requires ALPR searches be for a legitimate law enforcement purpose and prohibits improper uses, including discriminatory targeting, harassment, invasion of privacy, personal use, or any use that violates constitutional rights. SDPD's audits and public reporting are intended to reinforce accountability and reduce the risk of disproportionate impacts.

SDPD takes all community concerns seriously and continues working to strengthen its policies and practices to ensure ALPR technology is used responsibly to support public safety.

AUDITS OR INVESTIGATIONS

210.0102(a)(7) The results of any internal audits or internal investigations relating to surveillance technology, information about any violation of the Surveillance Use Policy, and any action taken in response. To the extent that the public release of this information is prohibited by law, City staff shall provide a confidential report to the City Council regarding this information to the extent allowed by law.

An ALPR system administrator, holding the supervisory rank of Sergeant, conducts weekly audits of the ALPR program. These audits ensure compliance with State and local laws, such as SB 34 and the TRUST Ordinance, SDPD's Use Policy, and proper system operation. The administrator verifies that all equipment is functioning correctly, data is not retained beyond the established retention period, and that all users with access have received the required training and authorization.

Each week, the audit also confirms that every search includes a valid and complete case or incident number in the "reason for search" field. The administrator checks that numbers are current, properly formatted, and not reused across multiple days or by multiple users. Although it is common for several officers to investigate the same case, resulting in multiple searches with the same case number, the administrator verifies that these searches are legitimate. This typically occurs during active incidents when multiple patrol officers are attempting to locate a suspect vehicle immediately after a crime. (Please see Addendum B for examples of such cases.)

The audit process also reviews for case numbers originating outside SDPD. Case numbers from other law enforcement agencies may appear in valid circumstances, such as when SDPD assists in a regional search or responds to California agency bulletins or wanted flyers. When this occurs, the system administrator confirms the request and verifies the validity of the search.

During the weekly audit process, four suspected violations of the Use Policy were identified.

Three violations involved invalid search reasons in the required case or event number metadata fields.

The other violation involved the sharing of ALPR data with an Arizona police department in connection with a criminal investigation.

Upon identifying the suspected violation, the user and their chain of command were notified immediately. The Department is investigating and will take further action, including discipline, if appropriate.

None of the suspected violations were related to immigration.

DATA BREACH OR UNAUTHORIZED ACCESS

210.0102(a)(8) 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, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the City.

There was no data breach or unauthorized access to SDPD ALPR data during 2025.

DATA BREACH DETECTION

210.0102(a)(9) A general description of all methodologies used to detect incidents of data breaches or unauthorized access, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the City.

Every week, a designated SDPD supervisor conducts a network audit that identifies whether any outside entities accessed the Department's ALPR system. Additionally, the ALPR vendor, Flock Safety, maintains a dedicated Risk and Compliance Department responsible for continuous monitoring of its systems to detect potential cybersecurity incidents or data breaches. In the event of a confirmed or suspected breach, Flock Safety is contractually required to immediately notify SDPD.

On top of these active methods for detecting unauthorized access, both the Department and the vendor rely on established cybersecurity best practices to reduce the risk of a breach occurring. All ALPR data is stored within the Amazon Government Cloud, which incorporates multiple layers of digital security.

The ALPR data itself is protected through encryption, firewalls, and multi-factor authentication, providing continuous safeguards against intrusion or compromise. Access to ALPR data is strictly limited to authorized SDPD personnel assigned to investigative or enforcement roles and approved by the Chief of Police.

ALPR data downloaded from a video management solution to a mobile workstation or to digital evidence storage (e.g., Axon Evidence) is only accessible through a City-controlled Single Sign-On (SSO), a password-protected system that logs every access by username, date, and time.

The SSO password must be reset at each login and follow strict complexity requirements:

1. At least 12 characters long.
2. Contain characters from at least three of the following categories:

    a. Uppercase letters (A–Z)
    b. Lowercase letters (a–z)
    c. Numbers (0–9)
    d. Symbols: ~ ! @ # $ % ^ & * ( ) - _

3. May not repeat any of the previous 24 passwords.
4. Cannot contain three or more identical characters in sequence.

Users must comply with all City computer security settings, including password expiration, complexity, and the automatic password-protected screen saver feature. Users are required to lock or log off when leaving a workstation with sensitive information visible.

Flock Safety also undergoes regular independent third-party audits and maintains multiple recognized cybersecurity certifications and compliance attestations, including SOC 2 Type II, ISO 27001:2022, NIST 800-53 / Rev. 5, and CJIS compliance, which provide additional oversight and validation of system security.

In 2023, prior to installation, the Flock ALPR solution underwent review through the Department of Information Technology's Governance Process and received full approval after demonstrating alignment with the City's technical and security standards. (See Addendum C for Flock Safety data security attestation.)

INFORMATION AND STATISTICS

210.0102(a)(10) Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes.

Qualitative and case-based evidence strongly demonstrates the effectiveness of ALPR technology.

In 2025, ALPR repeatedly helped officers solve crimes, locate suspects, connect inter-jurisdictional and multi-jurisdictional crimes, and recover stolen property with speed and accuracy. The technology assisted in 361 cases, including robberies, burglaries, rapes, sexual crimes against children and serious collisions.

ALPR technology was used to help solve nine of 28 homicides in 2025, contributing to a 96% solve rate.

The Department only logs an ALPR assist when the technology's use had a significant impact on the outcome of the investigation. For example, the system was used, without question, to positively identify a suspect vehicle or the system's Hotlist alerted officers to a wanted vehicle that resulted in the immediate apprehension of the suspect or vehicle. Successful

outcomes are evaluated and documented throughout the year by the system administrator to ensure accuracy and proper reporting.

While it is difficult to determine causation between specific crime trends and the implementation of ALPR, the data is encouraging. Motor vehicle thefts, one of the most directly impacted crime types, fell by more than 21 percent in the year the technology was installed and decreased another 22 percent in 2025. Thefts from motor vehicles also fell 25 percent in 2025. Overall, crime fell 6 percent across San Diego in 2025, which included decreases in nearly all major crime types.

Taken together, these examples illustrate that ALPR functions as a powerful investigative multiplier, helping officers focus on credible leads, preventing further victimization, and enhancing community safety while reducing the need for broad or intrusive patrol activity.

Quantitatively measuring the full impact of ALPR remains challenging. Because many baseline metrics had not been established before adopting ALPR, such as average case resolution time or officer hours spent per investigation, it is difficult to make precise comparisons between pre- and post-implementation outcomes. For example, investigators consistently report that ALPR dramatically reduces time spent identifying suspect vehicles and coordinating responses, but there is no pre-existing benchmark for how long these tasks took before the system was deployed.

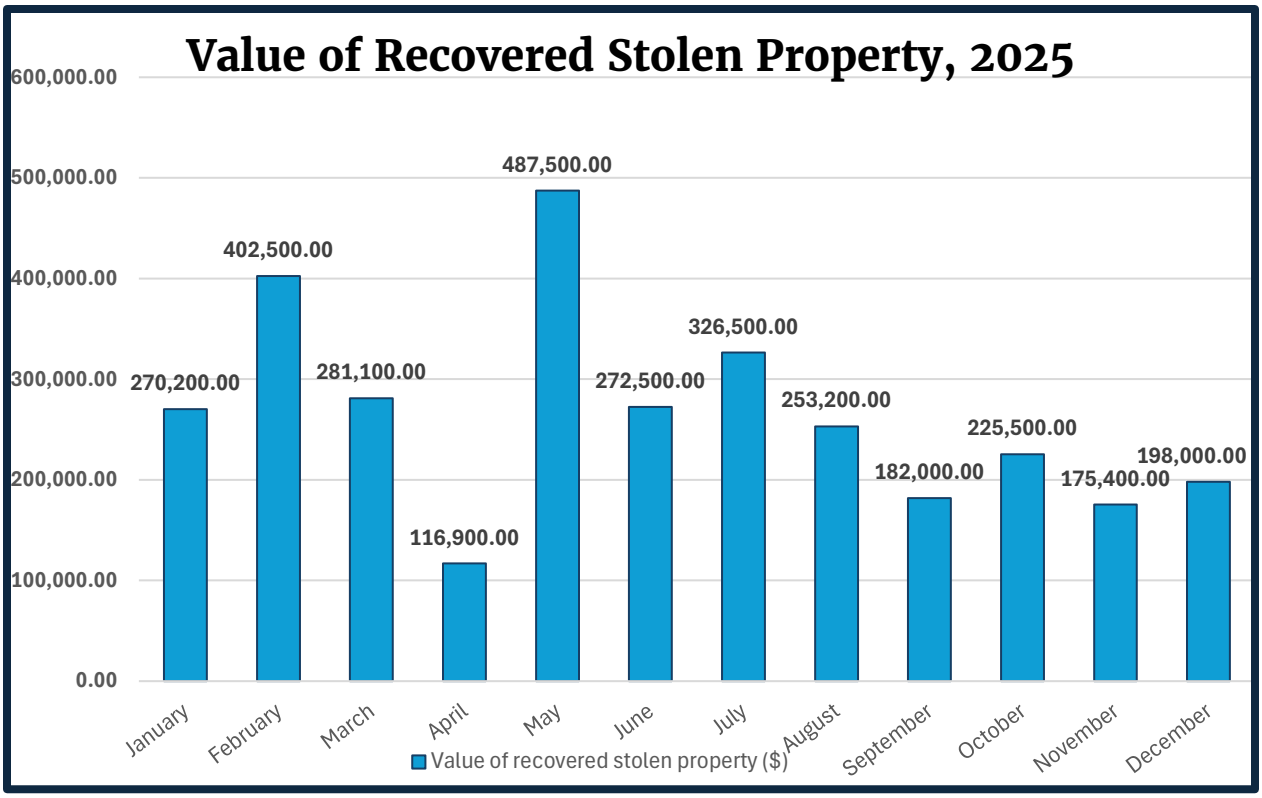
While future reports may include new performance benchmarks, the consistent outcomes across hundreds of investigations have demonstrated that ALPR technology is an indispensable, responsible, and effective tool in modern policing.

For additional performance metrics and detailed ALPR case examples, see Addendum B.

Investigative Highlights	
187 PC – Homicide	9
211 PC – Robbery	6
245 PC – Assault with a Deadly Weapon	5
261 PC – Rape	1
288 PC – Lewd or Lascivious Acts with a Child	1
459 – Burglary	15
Traffic (Serious Injury Crashes)	9
Missing Persons	4

Stolen Vehicle Assists	
Stolen Vehicles Recovered	259
Stolen Vehicle Suspects in Custody	199

Totals	
Total Assists	361
Total Suspect In Custody	269
Estimated Value of Recovered Stolen Property	$3,191,300
Recovered Guns	12



**Property value is based on the estimated value of stolen goods, like stolen vehicles.*

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

210.0102(a)(11) Statistics and information about California Public Records Act requests regarding the specific surveillance technology, including response rates, such as the number of California Public Records Act requests on the surveillance technology and the open and closed dates for each of these California Public Records Act requests.

There were 34 Public Records Act requests related to ALPR in calendar year 2025.

The information produced in response to those requests can be viewed on the City of San Diego's CPRA request portal: https://sandiego.nextrequest.com/

Request Number	Request Date	Closed Date
25-1132	2/10/2025	3/25/2025
25-2238	3/22/2025	3/27/2025
25-2949	4/15/2025	4/23/2025
25-2950	4/15/2025	4/22/2025
25-2639	4/4/2025	6/24/2025
25-4039	5/27/2025	6/17/2025
25-3837	5/19/2025	6/17/2025
25-4343	6/5/2025	6/26/2025
25-4858	6/26/2025	7/2/2025

Request Number (continued)	Request Date	Closed Date
25-5731	7/27/2025	7/29/2025
25-5752	7/28/2025	8/21/2025
25-6046	8/7/2025	8/15/2025
25-6087	8/10/2025	10/14/2025
25-6383	8/19/2025	8/29/2025
25-6387	8/19/2025	9/10/2025
25-6245	8/14/2025	9/10/2025
25-6415	8/20/2025	8/20/2025
25-6390	8/19/2025	11/17/2025
25-6445	8/20/2025	9/10/2025
25-6782	9/1/2025	6/26/2025
25-6890	9/4/2025	9/12/2025
25-7542	9/22/2025	OPEN
25-7847	10/6/2025	10/9/2025
25-7887	10/7/2025	10/21/2025
25-9108	11/14/2025	11/24/2025
25-8884	11/8/2025	11/20/2025
25-9626	12/3/2025	OPEN
25-9726	12/6/2025	12/17/2025
25-9807	12/8/2025	OPEN
25-9514	11/30/2025	12/11/2025
25-9844	12/10/2025	OPEN
25-9860	12/10/2025	OPEN
25-10137	12/18/2025	OPEN
25-10490	12/30/2025	12/31/2025

ANNUAL COST

210.0102(a)(12) Total annual costs for the surveillance technology, including any specific personnel-related and other ongoing costs, and what source will fund the surveillance technology in the coming year.

**These costs are duplicates of the Smart Streetlight (SSL) costs, as this is a partner technology, and the cost is built into the SSL costs.*

San Diego's Smart Streetlight system includes two partner technologies: situational awareness video cameras and ALPR cameras.

The annual service cost for the two integrated technologies is $2,012,500, based on a per-unit rate of $4,025.

Under the contract, all service fees are billed and paid in advance. On December 11, 2024, the City of San Diego paid the 2025 annual service fee.

Because not all 500 units were installed by the end of 2024, the vendor adjusted the fee to reflect the number of operational units, reducing the total from $2,012,500 to $1,449,602.08.

Additionally, the department paid for two (2) Smart Streetlight hubs that were damaged due to traffic collisions. The cost for both replacements was $8,000. The Department is working with City of San Diego Risk Management to recover these costs from the responsible parties.

All funding for the Smart Streetlight program was provided through the City's General Fund.

A copy of the full contract is available at cosd-public-safety-agreement-ubicquia.pdf.

REQUESTED MODIFICATIONS TO THE USE POLICY

210.0102(a)(13) Any requested modifications to the Surveillance Use Policy and a detailed basis for the request.

The following modifications were made to the ALPR Use Policy in collaboration with the PAB during the 2024 Annual Report review process:

- Add reference to California Senate Bill 34 under the subsection that defines prohibited ALPR uses, including those that violate federal, state or local laws.
- Clarify that ALPR data is stored consistent with the City's IT governance process.
- Add to the Third-Party Data Sharing section that ALPR data shall not be shared with private entities, out-of-state agencies, or federal agencies, including out-of-state and federal law enforcement agencies in accordance with SB 34.
- Replace references to "Special Projects and Legislative Affairs" & "SPLA" with "program administrator."
    - This change aligns with the new SDPD command structure.
- Remove section with header "Modifications to the Use Policy."
    - This change aligns this use policy with all other SDPD technology use policies. Modifications to a Surveillance Use Policy are governed by the Transparent and Responsible Use of Surveillance Technology Ordinance.
- Other additional typos and language corrections. These corrections do not impact the use of the technology.

These modifications to the Use Policy were approved by City Council on December 9, 2025. Those changes are memorialized in Resolution R-316544 dated December 12, 2025.

The following Use Policy changes are being proposed as part of the 2025 Annual Report review process:

- Prohibit conducting an ALPR search based solely on past arrests, detentions, or history of police interaction.
- Specify in the Data Access section that accessing ALPR outside of an employee's scheduled work hours is generally prohibited.
- Add to the Data Protection section a requirement that the Mayor and City Council will be notified of any data breach within 14 days.
- Other additional typos and language corrections. These corrections do not impact the use of technology.

ADDENDUM A – OUTSIDE AGENCY SHARING

HOW SDPD HANDLES ALPR SEARCH REQUESTS

SDPD does not grant outside agencies direct access to its ALPR system. When another California law enforcement agency needs assistance, they must contact SDPD, explain the qualifying reason for the request (such as a serious crime or public safety emergency), and then SDPD personnel conduct the search internally. The requesting agency is then informed of the relevant result, including whether no information was found. This type of sharing is legal under SB 34.

SEARCHES CONDUCTED BY SDPD FOR A CALIFORNIA AGENCY

California Agency	Times Shared
Burbank Police Department	1
Cal Fire	1
California Department of Corrections and Rehabilitation	1
California Department of Justice	1
California Highway Patrol	25
Carlsbad Police Department	8
Chula Vista Police Department	78
Coronado Police Department	2
Department of Motor Vehicles (CA) Investigators	4
East County Gang Task Force	2
El Cajon Police Department	55
Escondido Police Department	10
Glendale (CA) Police Department	2
Harbor Police Department	8
Human Trafficking Task Force	6
Internet Crimes against Children	10
La Mesa Police Department	35
Long Beach Police Department	2
Los Angeles County Sheriff's Office	1
Murietta Police Department	1
National City Police Department	37
Newport Beach Police Department	1
Oceanside Police Department	5
Pomona Police Department	1
Regional Auto Theft Task Force	9
San Bernardino County Sheriff's Office	1
San Diego Community College Police Department	1
San Diego County District Attorney Investigators	9
San Diego County Medical Examiner	1
San Diego County Sheriff's Office	133

California Agency (continued)	Times Shared
San Diego State University Police Department	13
San Francisco District Attorney CATCH	1
San Nicholas Police Department	2
Simi Valley Police Department	1
University of California San Diego Police Department	3
Violent Crimes Task Force	3

SEARCHES CONDUCTED BY SDPD FOR AN OUT-OF-STATE AGENCIES

Out-of-State Agency	Times Shared
Arizona Department of Public Safety	1
Goodyear (AZ) Police Department	1
New York Police Department	1
Portland Police Bureau	1

SEARCHES CONDUCTED BY SDPD FOR A FEDERAL AGENCY*

Federal/International Agency	Times Shared
Drug Enforcement Agency	17
Federal Bureau of Investigations/Joint Terrorism Task Force	2
Federal Probation	1
Homeland Security Investigations	3**
Narcotics Task Force	30

*None of these searches were for immigration-related cases.

**The three searches for Homeland Security Investigations were for two human trafficking cases, and one Internet Crimes Against Children (ICAC) case.

ADDENDUM B – EXPANDED METRICS AND CASE ILLUSTRATIONS

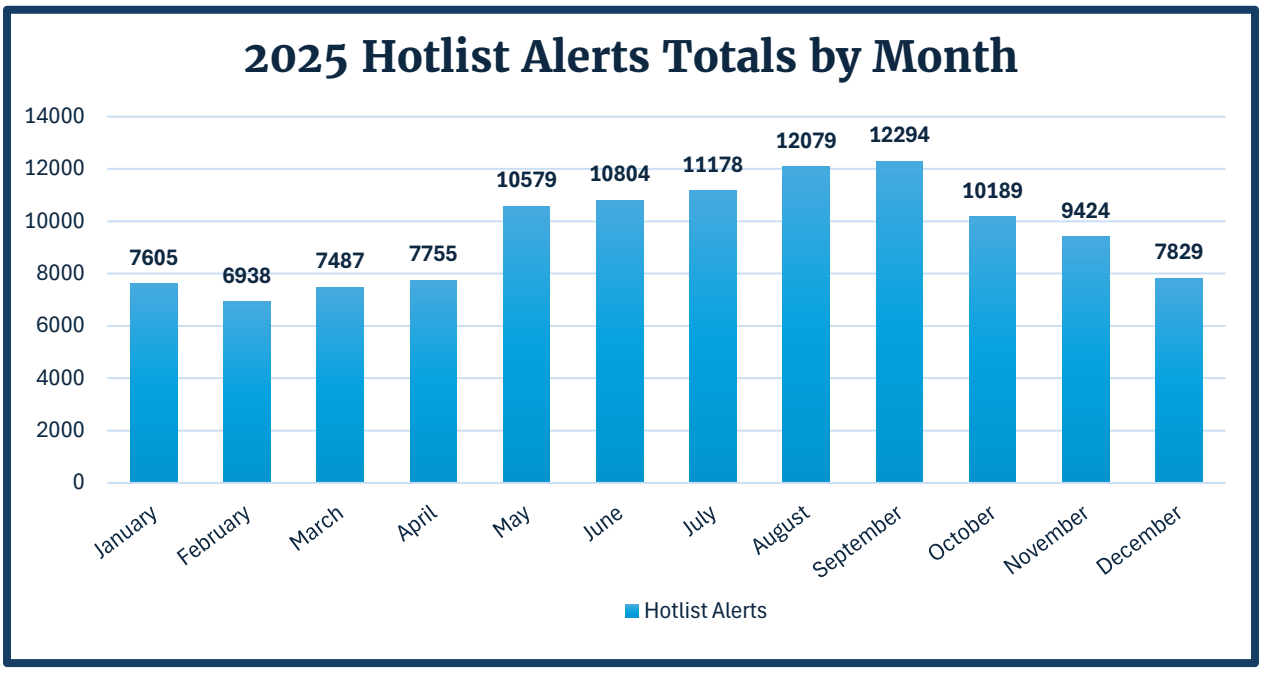
This addendum provides additional performance metrics and detailed case examples to further demonstrate the effectiveness of the ALPR system.

2025 HOTLIST TOTALS

A hotlist is a list of license plate numbers entered into the ALPR system that are linked to vehicles of interest to law enforcement. The hotlist enables officers to receive real-time alerts for stolen vehicles, vehicles with stolen or lost license plates, or vehicles connected to wanted suspects. The system is integrated with the National Crime Information Center (NCIC), which retrieves data from the Stolen Vehicle System and updates daily, ensuring that alerts are accurate and current. Alerts originating from the NCIC are classified as official hotlist alerts.

In addition to NCIC data, SDPD can add vehicles related to local investigations or at-risk individuals to a custom hotlist that is used only by SDPD. This allows officers to focus on vehicles specific to ongoing San Diego cases while still maintaining access to national information.

The 2025 Hotlist Alert Chart below shows the number of alerts received by SDPD each month. Each alert represents one of the following: a stolen vehicle, a stolen or lost license plate, a felony vehicle, or a custom hotlist entry associated with a local investigation.



113,385	*787*	*114,172*
2025 Official Hotlist Alerts	**2025 Custom Hotlist Alerts**	**2025 Total Hotlist Alerts**

109,840	3497	787	48
2025 Stolen License Plate Alerts	**2025 Stolen Vehicle Alerts**	**2025 Custom Hotlist Alerts**	**2025 Felony Vehicle Alerts**

JANUARY 2025

7511	94	7605
Official Hotlist Alerts	**Custom Hotlist Alerts**	**Total Hotlist Alerts**

January Investigation Highlights

187 PC - Homicide

On January 5, 2025, officers from the Department's Southeastern Division responded to a shooting near 300 Willie James Jones Avenue. Officers located a 19-year-old male in the street suffering from at least one gunshot wound to the torso. Officers administered first aid, and medics transported the male to a local hospital, where he later died.

Investigators determined two men were spray painting gang graffiti in the area and became involved in an altercation with the victim, during which he was shot. One suspect, a 21-year-old Latino male, was identified. An ALPR search helped identify and locate the suspect's vehicle, leading to his arrest. The second suspect remains outstanding, and the investigation is ongoing.

245 PC - Assault with a Deadly Weapon

On January 6, 2025, two males got into a fight at 5000 Newport Avenue. During the altercation, the suspect brandished a hatchet. The victim fled in a vehicle, and the suspect followed in his own vehicle. The suspect intentionally rammed the victim's vehicle multiple times during the chase through Ocean Beach. At one point, the suspect exited his vehicle, again brandished his hatchet, and swung it at the victim from approximately two to three feet away. As the suspect and victim drove away, the suspect crashed his vehicle into a parked Volvo and fled the scene.

Detectives requested that the suspect's vehicle be hot plated in the ALPR System. An ALPR hit alerted a detective, and the suspect was taken into custody. The suspect was sentenced to 365 days in jail.

FEBRUARY 2025

6,831	107	6,938
Official Hotlist Alerts	**Custom Hotlist Alerts**	**Total Hotlist Alerts**

February Investigation Highlight

10851 CVC - Vehicle Theft

On February 2, 2025, at about 9:20 p.m., officers received a stolen vehicle alert from the ALPR system and located it parked and occupied by a 38-year-old male. As officers conducted a high-risk traffic stop, the male fled in the vehicle, leading officers on a high-speed pursuit, swerving through traffic and driving on the wrong side of the road. The male eventually collided with another vehicle, fled on foot, and was taken into custody with the assistance of a police canine.

The suspect was arrested on suspicion of multiple crimes, including weapons and narcotics offenses, vehicle theft, evading police, identity theft and a parole violation. After court proceedings, the suspect was sentenced to seven years, four months in prison.

MARCH 2025

7,475	12	7,487
Official Hotlist Alerts	**Custom Hotlist Alerts**	**Total Hotlist Alerts**

March Investigation Highlights

20001 CVC - Felony Hit and Run

On March 29, 2025, a 31-year-old male riding an electric bicycle was fatally struck by two vehicles near 6900 Balboa Avenue. Both drivers fled the scene.

The Real Time Operations Center used Smart Streetlight camera footage and ALPR searches to identify the suspect vehicles, and a media release generated a corroborated tip.

Traffic investigators later identified both drivers. On July 2, 2025, both turned themselves in and were booked for felony hit-and-run. The male was sentenced to two years in prison, and the female was released on bond pending additional court proceedings.

187 PC - Homicide

On March 1st, 2025, officers were dispatched to a call regarding two males fighting. When officers arrived, they found a 61-year-old man gravely injured. Witnesses said the suspect strangled the victim and slammed his head against the ground.

The Real Time Operation Center pulled video from a nearby Smart Streetlight that captured the altercation and provided a description of the 55-year-old suspect, who was arrested soon after the incident. ALPR cameras helped lead detectives to a primary witness. The suspect is in custody pending further proceedings.

APRIL 2025

7,721	34	7,755
Official Hotlist Alerts	**Custom Hotlist Alerts**	**Total Hotlist Alerts**

April Investigation Highlights

487 PC - Grand Theft

Between March 24 and April 10, 2025, a male suspect stole multiple drive-thru headsets valued at several hundred to a thousand dollars each from Sonic, Arby's, and Carl's Jr. locations across San Diego. In each of the crimes, he fled in a dark-colored older-model BMW. The BMW was linked to the suspect through registration records and was placed on an SDPD hotlist. On April 16, 2025, an ALPR hit led officers to the suspect, who was arrested on suspicion of grand theft and four active misdemeanor warrants.

MAY 2025

10,511	68	10,579
Official Hotlist Alerts	Custom Hotlist Alerts	Total Hotlist Alerts

May Investigation Highlights

288 PC - Child Molest

While investigating a child molestation case, an SDPD detective used ALPR data to help prove a suspect was at the scene when the crime occurred. The suspect was ultimately taken into custody on suspicion of nine counts of lewd and lascivious acts with a child under 14 years old. The investigation, which is ongoing revealed there were 17 additional victims in Los Angeles County.

211 PC - Robbery

On May 20, 2025, SDPD Western Division officers investigated a robbery at the Days Inn on Hotel Circle South. Two victims reported a male and a female entered their hotel room with handguns and robbed them of their personal property.

A Real Time Operations Center detective received still images of surveillance footage showing the suspect vehicle, but the license plate was not visible due to image quality. Still, detectives were able to use other details from the images to search the Department's ALPR system, which led to the vehicle being identified.

On May 21, 2025, an ALPR camera captured the suspect vehicle driving on Imperial Avenue. Two hours later, Southeastern Patrol Officers located the vehicle and arrested the suspects. Both suspects are currently in custody awaiting sentencing.

JUNE 2025

10,704	*100*	*10,804*
Official Hotlist Alerts	**Custom Hotlist Alerts**	**Total Hotlist Alerts**

June Investigation Highlights

459 PC - Burglary

On May 27, 2025, a male and an unidentified accomplice used a white Nissan pickup truck to burglarize multiple cell tower equipment shelters, defeating entry alarms and stealing copper ground wire and equipment.

The burglaries occurred at AT&T sites on Adams Avenue, University Avenue, and Dalbergia Street, and at a T-Mobile site on Dalbergia Street. The losses were estimated to be in the thousands and exceeded an estimated $13,000 at two locations.

Investigators contacted RTOC for assistance identifying the suspect vehicle. Using ALPR data, RTOC identified the vehicle and placed it near the crime scenes. The suspect was later located and arrested for the four burglaries.

459 PC - Burglary

On June 6, 2025, a male drove a reported stolen vehicle to the RayzeBio business located on Morehouse Drive. The male broke open a box containing an access card, entered the building and stole multiple boxes and packages. Later that day, officers received an ALPR alert for the stolen vehicle located it near 2400 La Jolla Parkway. Investigators identified the driver as the RayzeBio burglary suspect, and stolen property was recovered from the vehicle.

The suspect was arrested and booked into jail. He pled guilty and is awaiting a review hearing.

JULY 2025

11,066	*112*	*11,178*
Official Hotlist Alerts	**Custom Hotlist Alerts**	**Total Hotlist Alerts**

July Investigation Highlights

261 PC - Rape

On July 14, 2025, a 19-year-old victim was held at gunpoint and assaulted by four suspects. During the incident, the suspects stole the victim's car keys and fled the area in the victim's vehicle. Officers responding to the radio call utilized ALPR data to quickly locate the stolen vehicle. All four suspects were subsequently detained and taken into custody without further incident. The case has been forwarded to the San Diego District Attorney's Office for prosecution.

245 PC - Assault with a Deadly Weapon

On July 24, 2025, officers responded to an assault with a deadly weapon involving a vehicle that left a victim with traumatic injuries. The RTOC reviewed Smart Streetlight camera footage and ALPR data, which positively identified the suspect vehicle. This information led to the arrest of the suspect in less than twelve hours. The case has been forwarded to the San Diego District Attorney's Office for prosecution.

AUGUST 2025

11,996	83	12,079
Official Hotlist Alerts	**Custom Hotlist Alerts**	**Total Hotlist Alerts**

August Investigation Highlights

220 PC - Assault with intent to commit Rape

In August of 2025, detectives investigated a series of sexual batteries targeting young women in University Heights, North Park, and Pacific Beach. The incidents initially lacked witnesses and available surveillance footage, making the identification of the suspect challenging. During the most recent incident, officers were able to locate and detain a potential suspect. The suspect was taken into custody and interviewed by detectives. Based on the information gathered during the interview, detectives reviewed ALPR data and were able to disprove the suspect's alibi. The case was forwarded to the San Diego City Attorney's Office for prosecution.

245 PC - Assault with a Deadly Weapon

On August 2, 2025, a victim was threatened with a firearm during a road-rage incident. The suspect fled the scene before officers could arrive. Responding officers obtained surveillance footage showing the suspect's license plate number. Using ALPR data, detectives located the suspect's vehicle. A search warrant was subsequently obtained for the suspect's residence, where detectives recovered two firearms. The suspect was arrested and booked into the San Diego County Central Jail on multiple charges.

SEPTEMBER 2025

12,250	44	12,294
Official Hotlist Alerts	**Custom Hotlist Alerts**	**Total Hotlist Alerts**

September Investigation Highlights

245 PC - Assault with a Deadly Weapon

On September 25, 2025, a vehicle registered to a suspect wanted in connection with an assault with a deadly weapon was entered into the Department's ALPR hot list. Ninety minutes later, the ALPR system alerted officers to the vehicle's location. Officers responded and took the suspect into custody without further incident.

OCTOBER 2025

10,138	51	10,189
Official Hotlist Alerts	**Custom Hotlist Alerts**	**Total Hotlist Alerts**

October Investigation Highlights

October

187 PC - Homicide

On October 18, 2025, detectives investigating a homicide in the Linda Vista area requested assistance from the RTOC) to help identify vehicles associated with the crime. RTOC detectives analyzed unique identifying characteristics of two vehicles of interest and matched them against ALPR data near the crime scene, allowing the vehicles to be positively identified. With this information, homicide detectives were able to identify multiple suspects connected to the crime. Arrests have been made, and court proceedings are currently underway.

211 PC - Robbery

On October 5, 2025, officers responded to a robbery involving a firearm. The reporting party provided a description of the suspect vehicle, which was immediately entered into the ALPR system. Officers quickly located a vehicle matching the description and initiated a traffic stop. Following a brief vehicle pursuit and a subsequent foot pursuit, the suspect was detained. After a positive witness identification, the suspect was taken into custody within three hours of the crime. The case has since been forwarded to the San Diego District Attorney's Office for prosecution.

NOVEMBER 2025

9,353	*71*	*9,424*
Official Hotlist Alerts	**Custom Hotlist Alerts**	**Total Hotlist Alerts**

November Investigation Highlights

245 PC - Assault with a Deadly Weapon

On November 13, 2025, the RTOC was monitoring police radio traffic when officers were dispatched to a violent assault with a rock. The suspect fled the scene in a vehicle, and a witness was able to provide the call taker with a vehicle description and a partial license plate number. Using the limited vehicle information available, RTOC conducted a search of the ALPR system and identified the suspect vehicle in the immediate area. This information was relayed to responding officers via police radio.

Officers located the suspect vehicle and took the suspect into custody within thirty minutes of the violent attack. The suspect was positively identified by witnesses and arrested for assault with a deadly weapon and an outstanding misdemeanor warrant for battery.

The victim sustained multiple head injuries and was transported to a local hospital for treatment. The case was submitted to the San Diego District Attorney's Office for review and prosecution.

245 PC - Assault with a Deadly Weapon

On November 19, 2025, detectives requested assistance from the RTOC in identifying a suspect vehicle involved in an assault with a deadly weapon. The suspect repeatedly struck the victim in the head with a glass bottle, causing severe injuries. During the investigation, surveillance footage was reviewed, however, the video quality was limited. Investigators noted the suspect vehicle had a unique and distinctive black hood.

Using the ALPR system, RTOC detectives successfully identified the suspect vehicle. A records check of the registered owner led investigators to an associate who was identified as the suspect in the attack. Within hours of the identification, officers had located and arrested the suspect.

DECEMBER 2025

7,829	11	7,840
Official Hotlist Alerts	**Custom Hotlist Alerts**	**Total Hotlist Alerts**

December Investigation Highlights

20001 CVC - Felony Hit and Run

On December 19, 2025, a pedestrian was struck while walking in a marked crosswalk by a white SUV. The vehicle fled the scene immediately following the collision. Responding officers arrived to find the victim unconscious and suffering from serious injuries. The RTOC promptly reviewed nearby Smart Street Light footage. Using this footage in combination with ALPR data, a RTOC detective was able to positively identify the suspect vehicle.

The information was quickly disseminated to officers in the field. Within hours, the suspect vehicle was located, and the driver was taken into custody for felony hit and run.

10851 CVC - Vehicle Theft

On December 23, 2025, patrol officers were alerted to the location of a stolen vehicle after an ALPR hit within their patrol beat. The officers responded and successfully located the vehicle occupied by two adults and two children. During the preliminary investigation, officers confirmed both adults were convicted felons. Furthermore, officers discovered an unserialized firearm inside the vehicle.

The adults were arrested on multiple charges including felon in possession of a firearm, felon in possession of ammunition, felon in possession of body armor, possessing a controlled substance while armed, possessing a controlled substance for sale, transporting a controlled substance, two counts of willful cruelty to a child, possession of a stolen vehicle and an outstanding warrant for narcotic sales. The children were removed from the situation and referred to the appropriate protective services.

ADDENDUM C – FLOCK Safety Inc. Data Security Attestation

To: San Diego City Council

From: Flock Safety | 1170 Howell Mill Road NW, Suite 104, Atlanta, GA 30318

Date: 1.22.26

Reference: San Diego Policy Advisory Board

Flock Safety attests to the following:

- Flock Safety currently is and has complied with the San Diego Police Department's (SDPD) Automatic License Plate Reader (ALPR) Use Policy.
- Flock Safety has not shared any SDPD ALPR data with any third party and no third party has accessed SDPD ALPR data, other than already reported in the ALPR Annual Surveillance Report.
- There have been no data breaches or other unauthorized access of SDPD's ALPR data.

Commitment to Security:

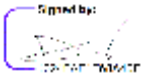
Flock Safety is committed to maintaining the highest standards of data security and privacy. Flock maintains policies on the use of ALPR data, security controls aligned with the NIST Cybersecurity Framework, and is certified to the following: SOC 2 Type II for Security and Availability, FedRAMP Authorization, ISO 27001 Security Management, and ISO 27701 Privacy Management certification. Flock also maintains operational procedures for the reporting of customer data loss events. Continuous internal assessments and audits are performed to confirm Flock's controls remain effective and aligned to these standards. We understand the importance of protecting the privacy and security of sensitive information and have taken and will continue to take measures aligned with industry-expected standards to mitigate the likelihood and impact of potential incidents. We are dedicated to the continuous improvement of our security posture.

Contact Information:

For any inquiries regarding this statement, please contact:

- Rob Otten, Senior Director, Risk and Compliance, Certified Information Systems Security Professional (CISSP) and Certified Information Privacy Professional - Technology (CIPP-T) @ robert.otten@flocksafety.com

Signature: **Date:**



1/22/2026

Dan Haley | Chief Legal Officer | Flock Safety

San Diego Police Department

Body Worn Camera (BWC)

Department/Division: Police – Operational Support

Related Policy/Procedure:

- DP 1.49 – Body Worn Cameras

DESCRIPTION

Body-Worn Cameras (BWCs) are used nationwide by law enforcement agencies to contemporaneously provide empirical evidence and create an objective audio and visual recording of a variety of encounters between the police and the public. BWCs are a vital tool in improving and enhancing the safety of officer and civilian interactions. BWC recordings facilitate review of events by supervisors, foster accountability, encourage lawful and respectful interactions between the public and the police, and may assist in de-escalation of possibly volatile encounters. Officers currently use the Axon Body 4 BWCs. SDPD seeks to balance the benefits provided by BWCs with the privacy rights of individuals who may be recorded during legal and procedurally just public interactions. Since the inception of the SDPD Body Worn Camera program in 2014, SDPD officers have recorded over eight million Body Worn Camera videos. During 2025, San Diego Police Department Officers recorded 707,321 body worn camera videos.

SHARING OF DATA

Approximately 20,000 "CASES" were created in Evidence.com in 2025 by investigators for the purpose of sharing with the District and City Attorneys. The "CASES" feature in Evidence.com allows investigators to organize all body worn camera videos in a specific folder. Those folders are then shared through the secured Axon Evidence.com website with the prosecutorial agency. Approximately 9,130 CASES were shared with the District Attorney's Office and approximately 10,807 with the City Attorney' Office. 3 CASES were also shared with the Riverside District Attorneys officer for prosecution.

CASES in Evidence.com were also shared with other law enforcement agencies to assist with criminal investigations. The following is a list of law enforcement agencies who San Diego Police Department shared CASES with in Evidence.com and how many cases were shared to each agency:

Agency	Number of cases
Escondido Police	1
Phoenix Police	1
Chula Vista Police	3
Harbor Police	2
El Cajon Police	1
Oceanside Police	2
National City Police	4
San Diego Unified School District Police	2

Agency (continued)	Number of cases
Carlsbad Police	1
Los Angeles County Sheriff's Department	1
La Mesa Police	4
California DOJ-Bureau of Investigations	7
Riverside County District Attorney	3
National City Police	4

In accordance with Senate Bill 1421, "certain peace officer or custodial officer personnel records and records relating to specified incidents, complaints, and investigations involving peace officers and custodial officers to be made available for public inspection pursuant to the California Public Records Act. The bill would define the scope of disclosable records." The body worn camera videos related to the "specified incidents" are redacted and posted on the City of San Diego's website www.sandiego.gov. Further disclosures may also be released in accordance with Senate Bill 16, regarding dishonesty, sexual assault, or other disclosable violations.

The San Diego Police Department receives subpoenas for body worn camera videos regarding civil litigation. After receiving the subpoena, the videos are shared through Evidence.com. In 2025 SDPD complied with approximately 250 civil subpoenas.

One (1) CASE in Evidence.com was shared with the California Commission on Peace Officer Standards and Training (POST).

LOCATION

Department Procedure 1.49 states, "Sworn personnel shall affix, by the BWC vendor-provided mounting device, the BWC on the frontmost portion of their torso, between the shoulders, below the collar, and above the waist. It shall be positioned on the outermost layer of clothing, such as the jacket, uniform shirt, or external vest cover, for maximum visual range an unobstructed view.

Members using a helmet BWC (e.g., SWAT, mounted) may position the BWC on the front of the helmet."

UPDATES, UPGRADES, AND CONFIGURATION CHANGES

The Axon Body Worn Cameras undergo monthly firmware updates which enables the cameras to continue operating efficiently and securely. In March of 2024, the San Diego Police Department integrated OKTA login with Evidence.com to better safeguard digital evidence from Cyber threats.

DEPLOYMENT LOCATION

The surveillance technology is worn by SDPD sworn personnel in all SDPD service areas throughout the City of San Diego.

COMMUNITY COMPLAINTS OR CONCERNS

The Department is committed to protecting civil rights and liberties of our citizens as presented to the City Council prior to approval of this technology. The Department has not

received any complaints or concerns about this surveillance technology or received any reports of disproportionate impacts. The Use Policy remains adequate to protect civil rights and civil liberties.

AUDITS OR INVESTIGATIONS

In response to the Privacy Advisory Board's (PAB) Memorandum addressed to San Diego City Council President LaCava and Members of the San Diego City Council on April 17, 2025, which provided a request for more rigorous auditing processes, the SDPD's Research, Analysis, and Planning Division published Department Order (OR) 25-13 on April 25, 2025. This order requires the managing unit (the managing unit is the person(s) recognized as the subject matter expert (SME) for the Transparent and Responsible Use of Surveillance Technology ordinance reporting or who controls the equipment) to prepare for the required Annual Report each year. The OR requires that the SMEs conduct quarterly audits of the equipment they are in charge of, including compiling and tracking information and data listed in SDMC 210.0102(a). On July 15, 2025, an additional Department Order, DO 25-23, was published. This DO requires Department members using any technology or database to enter a reference code/ID or justification for use of the technology or database with either a relevant full eight-digit case number, a full 11-digit event number, or other unique identification code. It requires that users no longer use nonspecific phrases or references and enhances the ability to audit the system.

In accordance with OR 25-13, and as an addition to the required quarterly audits by the managing unit, an independent audit was conducted by the Research, Analysis, and Planning Division (RAP)– Inspection and Control Unit. The audits were in addition to the quarterly audits required by the managing unit in OR 25-13. These audits targeted confirmation of the proper use of the technology, as stated in the Use Policy.

This technology was audited on 120 different case numbers, event numbers, or use statistics to verify the proper use of the technology. No unauthorized uses of the technology were located during the audit conducted by RAP.

Any substantial non-compliance or intentional misuse will be forwarded to the command or the Internal Affairs Unit for investigation and the subject may have their access permanently removed from the technology.

There was no unauthorized access of this technology and/or no located or reported violations of the Surveillance Use Policy or SDPD Policy or Procedure regarding this technology.

Any training issues or unintended input errors with this technology were identified and corrected. Continued errors or training issues will result in the user being suspended from the technology until they can be retrained on the technology.

Additionally, Sergeants and Detective Sergeants who have personnel assigned to them who wear a BWC are required to conduct monthly inspections. The inspections will ensure that the BWC is being used to record enforcement related contacts and other incidents set forth in this procedure. Inspection results will be entered and forwarded to the respective Lieutenant of the division for review and approval.

Sergeants and Detective Sergeants will randomly select at least two dates each month that their employees were working to inspect the proper use of their BWCs. Detective Sergeants will select days in which the BWCs were operationally used by their personnel. (It is possible the detectives will have no BWC recordings for that particular monthly inspection). The

supervisor will confirm that the number of enforcement contacts match up to the number of videos submitted. If the supervisor identifies a discrepancy, they will follow-up with the officer/detective to determine the reason the videos submitted did not match up with the number of contacts. If the supervisor is satisfied with the reason, no further action is required. If the supervisor feels a violation of this procedure occurred, appropriate action will be taken.

Sergeants and Detective Sergeants will make sure that all BWC videos were uploaded and categorized with the appropriate metadata. All videos that are uncategorized will be immediately corrected by the officer/detective. The supervisor will then re-inspect the BWC video to confirm the corrections were made.

Patrol Sergeants will select one video per day to inspect and verify the officer is in compliance with DP 1.49 (I) (1) (c) which states, "Officers shall begin recording in the Event Mode while driving to a call that has the potential to involve an enforcement contact". While viewing the video, Sergeants are reminded to use the "Post a note" function located below the video. Under the "Post a note" heading, Sergeants should enter "monthly inspection."

Employees Evidence.com accounts who are no longer employed with the department are deactivated. After the accounts are deactivated, the former employees no longer have access to view body worn camera digital evidence. The former employees are listed on a

"DEPARTED" list kept by the Operational Support Unit. The DEPARTED list is inspected on a monthly basis to insure all former employees no longer have access to Evidence.com.

There were no reported violations of the Surveillance Use Policy or SDPD Policy or Procedure regarding this technology.

DATA BREACH OR UNAUTHORIZED ACCESS

The City of San Diego's Department of Information Technology and SDPD Information Technology Unit has identified no data breaches or unauthorized access to the data collected by the surveillance technology.

DATA BREACH DETECTION

Axon Cloud Services system access control mechanisms are maintained in compliance with the specific Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) security requirements. BWC data is encrypted at rest and in transit. Axon maintains key management practices for managing the encryption keys. Axon maintains policies and practices for Axon Cloud Services that limit remote access to only authorized individuals and require at least wo factor for authentication. If a non-police officer/unauthorized user were to find a BWC in the field, the person would not be able to view the footage without Axon's proprietary viewer application, which has password protection.

The City's Department of Information Technology oversees the IT governance process and works with SDPD's Department of IT regarding project execution and risk assessment as well as selecting and approving technology solutions. Cyber security and technology risks are also assessed by the Department of IT. For additional details related to IT governance processes, refer to the information at the following link:

https://www.sandiego.gov/sites/default/files/fy23-fy27-it-strategic-plan-sd.pdf

INFORMATION AND STATISTICS

There are no direct relational crime statistics associated with or produced by the use of this technology.

Should the public want to access crime statistics for the City of San Diego, they can visit the City's *Crime Statistics & Crime Mapping* webpage: Crime Statistics & Crime Mapping | City of San Diego Official Website. The City's neighborhood crime summary dashboard is available at: San Diego Neighborhood Crime Dashboard (arcgis.com). A tab on this dashboard, Crime Data Explorer, allows the user to query crimes specific to a City neighborhood.

Additionally, crime data is also available on the City's Open Data Portal: Datasets - City of San Diego Open Data Portal. This crime data can be downloaded into usable files; also available on this site are dictionaries to help navigate the different data sets.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

There were 423 PRA Requests for this technology in 2025. The information produced in response to these requests can be viewed on the City of San Diego's CPRA request portal: https://sandiego.nextrequest.com/

Request Number	Requested Date	Closed Date
25-10402	12/28/2025	12/30/2025
25-10358	12/26/2025	01/05/2026
25-10368	12/23/2025	01/02/2026
25-10365	12/26/2025	01/02/2026
25-10360	12/26/2025	12/30/2026
25-10358	12/26/2025	01/05/2026
25-10347	12/25/2025	12/30/2026
25-10341	12/25/2025	12/30/2026
25-10335	12/24/2025	01/15/2026
25-10325	12/24/2025	01/07/2026
25-10291	12/23/2025	12/26/2025
25-10273	12/22/2025	12/26/2025
25-10270	12/21/2025	12/26/2025
25-10239	12/22/2025	12/26/2025
25-10238	12/22/2025	12/26/2025
25-10237	12/22/2025	12/26/2025
25-10213	12/21/2025	12/26/2025
25-10191	12/18/2025	12/26/2025
25-10161	12/17/2025	12/26/2025
25-10086	12/13/2025	12/24/2025

Request Number (continued)	Requested Date	Closed Date
25-10073	12/16/2025	01/22/2026
25-10070	12/16/2025	12/17/2025
25-10051	12/16/2025	01/14/2026
25-10017	12/16/2025	12/16/2025
25-10008	12/15/2025	Open
25-10004	12/15/2025	12/16/2025
25-9967	12/15/2025	12/15/2025
25-9964	12/14/2025	12/16/2025
25-9961	12/14/2025	12/16/2025
25-9960	12/14/2025	12/16/2025
25-9933	12/12/2025	12/22/2025
25-9926	12/12/2025	Open
25-9925	12/12/2025	01/05/2026
25-9838	12/09/2025	12/12/2025
25-9808	12/09/2025	12/09/2025
25-9806	12/08/2025	12/09/2025
25-9734	12/07/2025	12/09/2025
25-9729	12/06/2025	12/08/2025
25-9728	12/06/2025	12/17/2025
25-9719	12/06/2025	12/16/2025
25-9708	12/05/2025	12/15/2025
25-9692	12/05/2025	12/15/2025
25-9684	12/05/2025	12/15/2025
25-9661	12/04/2025	12/10/2025
25-9638	12/04/2025	12/04/2025
25-9637	12/04/2025	12/04/2025
25-9612	12/03/2025	12/09/2025
25-9603	12/03/2025	12/03/2025
25-9601	12/02/2025	12/04/2025
25-9556	12/02/2025	12/11/2025
25-9535	12/01/2025	12/02/2025
25-9521	12/01/2025	12/03/2025
25-9507	11/29/2025	12/09/2025
25-9455	11/27/2025	Open
25-9415	11/26/2025	11/28/2025

Request Number (continued)	Requested Date	Closed Date
25-9414	11/24/2025	11/25/2025
25-9377	11/24/2025	12/18/2025
25-9347	11/24/2025	Open
25-9341	11/23/2025	11/24/2025
25-9340	11/23/2025	11/24/2025
25-9388	11/23/2025	12/04/2025
25-9335	11/23/2025	11/24/2025
25-9334	11/23/2025	11/24/2025
25-9331	11/22/2025	11/24/2025
25-9326	11/22/2025	Open
25-9311	11/21/2025	11/26/2025
25-9309	11/21/2025	12/15/2025
25-9283	11/20/2025	Open
25-9281	11/20/2025	11/20/2025
25-9269	11/20/2025	11/20/2025
25-9253	11/20/2025	11/20/2025
25-9176	11/17/2025	11/25/2025
25-9165	11/17/2025	11/20/2025
25-9120	11/16/2025	11/18/2025
25-9017	11/12/2025	11/24/2025
25-9110	11/15/2025	11/18/2025
25-9041	11/13/2025	11/17/2025
25-9024	11/12/2025	11/21/2025
25-9017	11/12/2025	11/24/2025
25-8982	11/12/2025	11/12/2025
25-8975	11/11/2025	11/13/2025
25-8912	11/10/2025	11/12/2025
25-8903	11/10/2025	11/12/2025
25-8875	11/08/2025	11/10/2025
25-8874	11/07/2025	11/12/2025
25-8871	11/07/2025	12/11/2025

Request Number (continued)	Requested Date	Closed Date
25-8844	11/07/2025	11/17/2025
25-8841	11/07/2025	11/07/2025
25-8833	11/06/2025	11/13/2025
25-8828	11/06/2025	12/16/2025
25-8766	11/05/2025	11/14/2025
25-8763	11/05/2025	11/05/2025
25-8736	11/04/2025	11/19/2025
25-8710	11/04/2025	11/04/2025
25-8649	11/03/2025	11/04/2025
25-8635	11/02/2025	11/12/2025
25-8632	11/01/2025	Open
25-8631	11/01/2025	11/04/2025
25-8622	10/31/2025	12/26/2025
25-8594	10/30/2025	10/31/2025
25-8555	10/29/2025	10/30/2025
25-8522	10/28/2025	10/29/2025
25-8499	10/28/2025	11/28/2025
25-8498	10/28/2025	10/29/2025
25-8493	10/28/2025	12/17/2025
25-8434	10/26/2025	10/30/2025
25-8389	10/24/2025	10/24/2025
25-8336	10/22/2025	10/23/2025
25-8334	10/22/2025	10/23/2025
25-8333	10/22/2025	10/30/2025
25-8332	10/22/2025	11/06/2025
25-8327	10/22/2025	10/29/2025
25-8313	10/22/2025	10/23/2025
25-8291	10/21/2025	10/21/2025
25-8236	10/20/2025	10/21/2025
25-8134	10/15/2025	10/16/2025
25-8133	10/15/2025	10/16/2025

Request Number (continued)	Requested Date	Closed Date
25-8086	10/14/2025	10/16/2025
25-8066	10/13/2025	10/14/2025
25-8035	10/13/2025	10/13/2025
25-7998	10/11/2025	10/13/2025
25-7992	10/10/2025	10/20/2025
25-7952	10/09/2025	10/14/2025
25-7949	10/09/2025	10/09/2025
25-7919	10/08/2025	10/08/2025
25-7901	10/08/2025	10/08/2025
25-7889	10/07/2025	10/08/2025
25-7884	10/07/2025	10/08/2025
25-7868	10/07/2025	10/08/2025
25-7859	10/07/2025	10/07/2025
25-7858	10/07/2025	11/02/2025
25-7855	10/07/2025	10/07/2025
25-7840	10/06/2025	10/14/2025
25-7831	10/06/2025	10/07/2025
25-7823	10/06/2025	Open
25-7822	10/06/2025	Open
25-7821	10/06/2025	10/06/2025
25-7820	10/06/2025	10/16/2025
25-7819	10/06/2025	10/07/2025
25-7818	10/06/2025	Open
25-7807	10/05/2025	10/15/2025
25-7806	10/05/2025	10/15/2025
25-7805	10/05/2025	10/15/2025
25-7804	10/05/2025	10/15/2025
25-7803	10/05/2025	10/15/2025
25-7802	10/05/2025	10/15/2025
25-7801	10/05/2025	10/15/2025
25-7800	10/02/2025	10/03/2025

Request Number (continued)	Requested Date	Closed Date
25-7730	10/02/2025	10/07/2025
25-7720	10/02/2025	10/03/2025
25-7702	10/01/2025	10/08/2025
25-7685	10/01/2025	10/15/2025
25-7646	09/30/2025	10/10/2025
25-7637	09/29/2025	10/08/2025
25-7632	09/29/2025	09/30/2025
25-7553	09/27/2025	09/29/2025
25-7526	09/26/2025	09/30/2025
25-7519	09/26/2025	09/26/2025
25-7518	09/26/2025	09/26/2025
25-7515	09/25/2025	10/07/2025
25-7506	09/25/2025	09/26/2025
25-7473	09/24/2025	10/16/2025
25-7466	09/24/2025	10/03/2025
25-7448	09/24/2025	11/14/2025
25-7421	09/23/2025	10/02/2025
25-7420	09/23/2025	09/24/2025
25-7415	09/23/2025	10/02/2025
25-7413	09/23/2025	10/01/2025
25-7328	09/19/2025	09/22/2025
25-7322	09/19/2025	09/23/2025
25-7293	09/18/2025	09/19/2025
25-7275	09/18/2025	09/23/2025
25-7269	09/18/2025	09/18/2025
25-7268	09/18/2025	09/18/2025
25-7267	09/18/2025	09/18/2025
25-7266	09/18/2025	10/10/2025
25-7265	09/18/2025	10/01/2025
25-7264	09/18/2025	10/07/2025
25-7263	09/17/2025	10/01/2025

Request Number (continued)	Requested Date	Closed Date
25-7230	09/16/2025	09/17/2025
25-7202	09/16/2025	Open
25-7191	09/16/2025	09/16/2025
25-7190	09/16/2025	09/17/2025
25-7189	09/16/2025	09/26/2025
25-7188	09/16/2025	09/26/2025
25-7187	09/16/2025	09/26/2025
25-7186	09/16/2025	09/26/2025
25-7185	09/16/2025	09/26/2025
25-7184	09/16/2025	09/26/2025
25-7183	09/16/2025	09/26/2025
25-7182	09/16/2025	09/27/2025
25-7181	09/15/2025	09/66/2025
25-7120	09/12/2025	09/22/2025
25-7119	09/12/2025	09/12/2025
25-7105	09/12/2025	09/22/2025
25-7102	09/11/2025	09/29/2025
25-7101	09/11/2025	10/13/2025
25-7100	09/11/2025	09/29/2025
25-7099	09/11/2025	10/02/2025
25-7098	09/11/2025	09/12/2025
25-7097	09/11/2025	10/02/2025
25-7079	09/11/2025	09/16/2025
25-7076	09/11/2025	09/11/2025
25-7072	09/11/2025	09/11/2025
25-7030	09/10/2025	09/10/2025
25-7019	09/09/2025	09/15/2025
25-6997	09/09/2025	09/10/2025
25-6993	09/08/2025	09/10/2025
25-6967	09/08/2025	09/09/2025
25-6963	09/08/2025	09/12/2025

Request Number (continued)	Requested Date	Closed Date
25-6959	09/07/2025	11/06/2025
25-6956	09/06/2025	09/08/2025
25-6949	09/06/2025	09/15/2025
25-6923	09/05/2025	09/29/2025
25-6907	09/04/2025	09/08/2025
25-6891	09/04/2025	09/05/2025
25-6887	09/03/2025	09/05/2025
25-6860	09/04/2025	09/10/2025
25-6853	09/03/2025	09/17/2025
25-6835	09/03/2025	09/04/2025
25-6834	09/03/2025	09/10/2025
25-6833	09/03/2025	09/03/2025
25-6821	09/02/2025	09/03/2025
25-6792	09/02/2025	09/02/2025
25-6778	09/01/2025	09/10/2025
25-6765	08/31/2025	09/02/2025
25-6760	08/31/2025	09/02/2025
25-6694	08/28/2025	08/28/2025
25-6661	08/27/2025	08/27/2025
25-6526	08/23/2025	08/28/2025
25-6503	08/22/2025	09/12/2025
25-6481	08/21/2025	08/26/2025
25-6424	08/20/2025	08/29/2025
25-6409	08/20/2025	08/29/2025
25-6406	08/19/2025	08/20/2025
25-6405	08/19/2025	08/20/2025
25-6382	08/19/2025	08/28/2025
25-6334	08/18/2025	08/27/2025
25-6308	08/18/2025	09/19/2025
25-6244	08/14/2025	08/21/2025
25-6235	08/14/2025	09/24/2025

Request Number (continued)	Requested Date	Closed Date
25-6132	08/11/2025	09/18/2025
25-6131	08/11/2025	08/20/2025
25-6130	08/11/2025	09/18/2025
25-6129	08/11/2025	08/19/2025
25-6128	08/11/2025	08/20/2025
25-6127	08/11/2025	08/19/2025
25-6126	08/11/2025	09/18/2025
25-6122	8/11/2025	08/21/2025
25-6110	8/11/2025	8/11/2025
25-6104	08/11/2025	08/21/2025
25-6089	08/10/2025	08/12/2025
25-6080	08/09/2025	09/04/2025
25-6076	08/09/2025	08/20/2025
25-6075	08/09/2025	08/12/2025
25-6074	08/09/2025	08/21/2025
25-6038	08/07/2025	08/15/2025
25-6032	08/07/2025	08/15/2025
25-6024	08/07/2025	08/15/2025
25-5914	08/03/2025	08/12/2025
25-5912	08/02/2025	08/13/2025
25-5911	08/02/2025	08/05/2025
25-5830	07/30/2025	08/05/2025
25-5827	07/30/2025	07/31/2025
25-5815	07/29/2025	07/30/2025
25-5783	07/29/2025	08/14/2025
25-5782	07/29/2025	08/14/2025
25-5728	07/27/2025	07/28/2025
25-5720	07/27/2025	08/05/2025
25-5710	07/26/2025	08/07/2025
25-5705	07/26/2025	07/28/2025
25-5680	07/24/2025	07/28/2025

Request Number (continued)	Requested Date	Closed Date
25-5566	07/22/2025	08/15/2025
25-5605	07/22/2025	07/23/2025
25-5550	07/21/2025	07/24/2025
25-5544	07/21/2025	07/23/2025
25-5541	07/21/2025	07/23/2025
25-5531	07/21/2025	07/29/2025
25-5483	07/17/2025	07/18/2025
25-5476	07/17/2025	07/18/2025
25-5441	07/16/2025	07/17/2025
25-5429	07/16/2025	07/30/2025
25-5414	07/15/2025	08/15/2025
25-5390	07/15/2025	07/15/2025
25-5369	07/14/2025	07/17/2025
25-5331	07/14/2025	07/16/2025
25-5272	07/11/2025	07/14/2025
25-5226	07/09/2025	Open
25-5138	07/07/2025	07/14/2025
25-5116	07/06/2025	07/08/2025
25-5115	07/06/2025	07/07/2025
25-5097	07/05/2025	07/08/2025
25-5043	07/02/2025	07/03/2025
25-5003	07/01/2025	08/13/2025
25-5002	07/01/2025	08/08/2025
25-5000	07/01/2025	07/08/2025
25-4979	07/01/2025	07/01/2025
25-4921	06/29/2025	06/30/2025
25-4906	06/27/2025	07/01/2025
25-4872	06/26/2025	06/26/2025
25-4866	06/26/2025	06/26/2025
25-4821	06/24/2025	07/01/2025
25-4816	06/24/2025	07/09/2025

Request Number (continued)	Requested Date	Closed Date
25-4778	06/23/2025	Open
25-4753	06/23/2025	06/24/2025
25-4742	06/21/2025	07/09/2025
25-4575	06/15/2025	06/16/2025
25-4574	06/15/2025	06/16/2025
25-4564	06/14/2025	06/23/2025
25-4528	06/12/2025	06/13/2025
25-4527	06/12/2025	06/13/2025
25-4522	06/12/2025	06/12/2025
25-4511	06/12/2025	06/12/2025
25-4510	06/12/2025	06/18/2025
25-4475	06/10/2025	06/18/2025
25-4473	06/10/2025	06/18/2025
25-4437	06/10/2025	06/11/2025
25-4429	06/09/2025	06/10/2025
25-4347	06/06/2025	06/09/2025
25-4311	06/04/2025	06/05/2025
25-4247	06/03/2025	06/03/2025
25-4195	06/01/2025	06/13/2025
25-4192	05/31/2025	06/02/2025
25-4170	05/30/2025	06/05/2025
25-4144	05/29/2025	05/30/2025
25-4104	05/28/2025	05/29/2025
25-4057	05/27/2025	05/28/2025
25-3983	05/24/2025	05/30/2025
25-3944	05/22/2025	05/23/2025
25-3922	05/22/2025	05/28/2025
25-3920	05/21/2025	05/22/2025
25-3918	05/21/2025	05/22/2025
25-3889	05/20/2025	05/21/2025
25-3886	05/20/2025	05/21/2025

Request Number (continued)	Requested Date	Closed Date
25-3814	05/18/2025	05/19/2025
25-3739	05/15/2025	07/23/2025
25-3729	05/15/2025	05/15/2025
25-3686	05/14/2025	07/09/2025
25-3590	05/09/2025	05/09/2025
25-3581	05/09/2025	05/13/2025
25-3527	05/08/2025	07/10/2025
25-3440	05/05/2025	05/05/2025
25-3369	05/01/2025	05/07/2025
25-3252	04/28/2025	04/28/2025
25-3172	04/24/2025	04/24/2025
25-3170	04/24/2025	04/24/2025
25-3060	04/19/2025	04/22/2025
25-3059	04/19/2025	04/22/2025
25-3047	04/18/2025	04/24/2025
25-2939	04/15/2025	12/11/2025
25-2874	04/13/2025	04/24/2025
25-2873	04/13/2025	Open
25-2860	04/11/2025	04/14/2025
25-2834	04/10/2025	04/11/2025
25-2824	04/10/2025	04/11/2025
25-2774	04/09/2025	04/17/2025
25-2750	04/08/2025	04/18/2025
25-2743	04/08/2025	09/09/2025
25-2705	04/07/2025	04/08/2025
25-2351	03/26/2025	Open
25-2343	03/26/2025	03/26/2025
25-2233	03/22/2025	04/02/2025
25-2205	03/21/2025	03/26/2025
25-2152	03/19/2025	03/20/2025
25-2127	03/19/2025	03/19/2025

Request Number (continued)	Requested Date	Closed Date
25-2081	03/17/2025	03/27/2025
25-2046	03/16/2025	03/17/2025
25-2039	03/15/2025	03/17/2025
25-2012	03/14/2025	03/25/2025
25-2005	03/14/2025	03/14/2025
25-1950	03/12/2025	03/21/2025
25-1878	03/11/2025	06/18/2025
25-1789	03/07/2025	03/11/2025
25-1745	03/05/2025	Open
25-1702	03/04/2025	03/06/2025
25-1599	02/27/2025	03/06/2025
25-1539	02/25/2025	06/27/2025
25-1534	02/24/2025	03/06/2025
25-1473	02/24/2025	02/25/2025
25-1348	02/19/2025	02/20/2025
25-1311	02/18/2025	02/18/2025
25-1310	02/18/2025	02/18/2025
25-1289	02/18/2025	02/18/2025
25-1288	02/18/2025	04/22/2025
25-1227	02/05/2025	02/13/2025
25-1009	02/05/2025	02/27/2025
25-1008	02/05/2025	02/06/2025
25-885	02/03/2025	02/03/2025
25-692	01/27/2025	01/28/2025
25-663	01/27/2025	01/27/2025
25-655	01/26/2025	01/29/2025
25-621	01/25/2025	01/27/2025
25-528	01/22/2025	02/20/2025

ANNUAL COST

The cost for 2025 is $2,331,868.48. The cost for 2026 is $2,386,238.89.

This cost is funded through the state COPS fund.

REQUESTED MODIFICATIONS TO THE USE POLICY

There were no requested modifications to the Body Worn Camera Procedure.

San Diego Police Department

Smart Streetlights (SSL)

Department/Division: Police – Real Time Operations Center (RTOC)

Related Policy/Procedure:

- DP 3.33 Smart Streetlight System
- DP 3.02 Property and Evidence

DESCRIPTION

210.0102(a)(1) A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the surveillance technology.

The San Diego Police Department used video evidence, along with data and information from authorized technologies embedded within Smart Streetlights (SSL) over 2,800 times, to conduct criminal investigations against persons and property and internal investigations. Additionally, video obtained from the Smart Streetlights was used to investigate fatal traffic collisions, providing a clear understanding of how events unfolded.

SHARING OF DATA

210.0102(a)(2) Whether and how often data acquired through the use of the surveillance technology was shared with any non-City entities, the name of any recipient entity, the types of data disclosed, under what legal standards the information was disclosed, and the justification for the disclosure, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the City.

In addition to providing Smart Streetlight data to the District Attorney's/City Attorney's Office for criminal prosecution, video evidence and data was accessed by SDPD personnel and disclosed to other law enforcement agencies only after a qualifying crime had taken place (e.g., homicide or shooting) and only when a legitimate investigative need existed. These were the instances where data was shared to other law enforcement agencies:

Agency Shared With	Times Shared
California Highway Patrol	4
San Diego Community College District PD	2
San Diego Unified Schools PD	1

LOCATION

210.0102(a)(3) A description of the physical objects to which the surveillance technology hardware was installed, if applicable, and without revealing the specific location of the hardware, and a breakdown of the data sources applied or related to the surveillance technology software.

The Smart Streetlights with embedded ALPR technology were attached to City of San Diego streetlight poles.

UPDATES, UPGRADES, AND CONFIGURATION CHANGES

210.0102(a)(4) A list of the software updates, hardware upgrades, and system configuration changes that expanded or reduced the surveillance technology capabilities, as well as a description of the reason for the changes, except that no confidential or sensitive information should be disclosed that would violate any applicable law or undermine the legitimate security interests of the City.

There have been no updates, upgrades, or configuration changes in 2025.

DEPLOYMENT LOCATION

210.0102(a)(5) A description of where the surveillance technology was deployed geographically, by each City Council District or police area, in the applicable year.

The cameras were deployed Citywide in all police divisions.

Current camera deployment locations can be found at the link below.

- https://webmaps.sandiego.gov/portal/apps/webappviewer/index.html

COMMUNITY COMPLAINTS OR CONCERNS

210.0102(a)(6) A summary of any community complaints or concerns about the surveillance technology and an analysis of its Surveillance Use Policy, including whether it is adequate in protecting civil rights and civil liberties, and whether, and to what extent, the use of the surveillance technology disproportionately impacts certain groups or individuals.

The Department is committed to protecting the civil rights and liberties of our citizens, as presented to the City Council prior to approval of this technology. The department has not received any complaints or concerns about this surveillance technology or received any reports of disproportionate impacts. The Use Policy continues to protect civil rights and civil liberties.

AUDITS OR INVESTIGATIONS

210.0102(a)(7) The results of any internal audits or internal investigations relating to surveillance technology, information about any violation of the Surveillance Use Policy, and any action taken in response. To the extent that the public release of this information is prohibited by law, City staff shall provide a confidential report to the City Council regarding this information to the extent allowed by law.

An audit was completed in accordance with Department Order 25-13. There was no unauthorized access to this technology.

Monthly audits were conducted, and no violations of the Use Policy were identified.

DATA BREACH OR UNAUTHORIZED ACCESS

210.0102(a)(8) 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, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the City.

There were no data breaches or unauthorized access to the data collected by the surveillance technology.

DATA BREACH DETECTION

210.0102(a)(9) A general description of all methodologies used to detect incidents of data breaches or unauthorized access, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the City.

The City's Department of Information Technology oversees the IT governance process and works with SDPD's Department of IT regarding project execution and risk assessment, selecting, and approving technology solutions. Cyber security and technology risks are also assessed by the Department of IT. For additional details related to IT governance processes, refer to the information at the following link:

- https://www.sandiego.gov/sites/default/files/fy23-fy27-it-strategic-plan-sd.pdf

INFORMATION AND STATISTICS

210.0102(a)(10) Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes.

SSL videos were utilized for investigations 2,822 times during 2025.

Should the public want to access crime statistics for the City of San Diego, they can visit the City's *Crime Statistics & Crime Mapping* webpage: Crime Statistics & Crime Mapping | City of San Diego Official Website. Accessible via this webpage is the City's neighborhood crime summary dashboard: San Diego Neighborhood Crime Dashboard (arcgis.com). A tab on this dashboard, Crime Data Explorer, allows the user to query crimes specific to a City neighborhood.

Additionally, crime data is also available on the City's Open Data Portal: Datasets - City of San Diego Open Data Portal. This crime data can be downloaded into usable files; also available on this site are dictionaries to help navigate the different data sets.

PUBLIC RECORDS ACT REQUESTS

210.0102(a)(11) Statistics and information about California Public Records Act requests regarding the specific surveillance technology, including response rates, such as the number of California Public Records Act requests on the surveillance technology and the open and closed dates for each of these California Public Records Act requests.

There were 177 Public Records Act requests regarding this technology in 2025.

The information produced in response to those requests can be viewed on the City of San Diego's CPRA request portal: https://sandiego.nextrequest.com/

Request Number	Request Date	Closed Date
25-266	1/13/2025	1/13/2025
25-309	1/14/2025	1/14/2025
25-348	1/15/2025	1/17/2025
25-470	1/20/2025	1/21/2025
25-643	1/26/2025	1/27/2025
25-837	1/31/2025	2/3/2025
25-977	2/5/2025	2/12/2025
25-1037	2/6/2025	2/7/2025
25-1081	2/7/2025	2/11/2025
25-869	2/2/2025	2/11/2025
25-1380	2/20/2025	2/21/2025
25-1386	2/20/2025	2/28/2025
25-1388	2/20/2025	2/21/2025
25-1499	2/24/2025	3/4/2025
25-1604	2/28/2025	2/28/2025
25-1637	3/1/2025	3/3/2025
25-1735	3/5/2025	3/5/2025
25-1747	3/6/2025	3/6/2025
25-1847	3/10/2025	3/11/2025
25-1923	3/12/2025	3/12/2025
25-2131	3/19/2025	3/19/2025
25-2265	3/24/2025	3/24/2025
25-2433	3/28/2025	4/2/2025
25-2431	3/28/2025	4/2/2025
25-2453	3/29/25	4/2/2025
25-2565	4/2/2025	4/14/2025
25-2570	4/2/2025	4/2/2025
25-2582	4/2/2025	4/3/2025
25-2564	4/2/2025	4/3/2025
25-2836	4/10/2025	4/11/2025
25-2934	4/15/2025	4/15/2025
25-3054	4/18/2025	4/21/2025
25-3223	4/26/2025	4/29/2025
25-3583	5/9/2025	5/12/2025

Request Number (continued)	Request Date	Closed Date
25-3642	5/12/2025	5/13/2025
25-3643	5/12/2025	5/14/2025
25-3957	5/23/2025	5/27/2025
25-3995	5/25/2025	5/27/2025
25-3455	5/4/2025	6/11/2025
25-3960	5/23/2025	5/28/2025
25-4215	6/2/2025	6/3/2025
25-4214	6/2/2025	6/3/2025
25-4328	6/5/2025	6/5/2025
25-4362	6/6/2025	6/9/2025
25-4472	6/10/2025	6/12/2025
25-4509	6/12/2025	6/12/2025
25-4540	6/13/2025	6/13/2025
25-4573	6/14/2025	6/17/2025
25-4599	6/16/2025	6/17/2025
25-4729	6/20/2025	6/23/2025
25-4773	6/23/2025	6/24/2025
25-4824	6/25/2025	6/26/2025
25-4888	6/26/2025	7/1/2025
25-4917	6/28/2025	7/1/2025
25-4979	7/1/2025	7/1/2025
25-5139	7/7/2025	7/8/2025
25-4888	6/26/2025	7/1/2025
25-5079	7/3/2025	7/8/2025
25-5073	7/3/2025	7/9/2025
25-5206	7/9/2025	7/9/2025
25-5253	7/10/2025	7/11/2025
25-5286	7/11/2025	7/14/2025
25-5526	7/21/2025	7/22/2025
25-5532	7/21/2025	7/22/2025
25/5528	7/21/2025	7/22/2025
25-5725	7/27/2025	7/29/2025
25-5731	7/27/2025	7/29/2025
25-5946	8/4/2025	8/8/2025
25-5954	8/5/2025	8/5/2025
25-5955	8/5/2025	8/6/2025

Request Number (continued)	Request Date	Closed Date
25-5986	8/6/2025	8/6/2025
25-6000	8/6/2025	8/6/2025
25-6113	8/11/2025	8/13/2025
25-6127	8/11/2025	8/19/2025
25-6129	8/11/2025	8/19/2025
25-6131	8/11/2025	8/20/2025
25-6126	8/11/2025	9/18/2025
25-6128	8/11/2025	8/20/2025
25-6130	8/11/2025	9/18/2025
25-6132	8/11/2025	9/18/2025
25-6182	8/12/2025	8/19/2025
25-6044	8/7/2025	8/14/2025
25-6246	8/14/2025	8/15/2025
25-6256	8/14/2025	8/15/2025
25-6271	8/15/2025	8/15/2025
25-6357	8/18/2025	8/19/2025
25-6087	8/10/2025	10/14/2025
25-6434	8/20/2025	8/21/2025
25-6449	8/20/2025	8/21/2025
25-6453	8/20/2025	8/21/2025
25-6468	8/21/2025	8/22/2025
25-6557	8/25/2025	8/26/2025
25-6738	8/29/2025	9/2/2025
25-6786	9/2/2025	9/2/2025
25-6869	9/4/2025	9/4/2025
25-7015	9/9/2025	9/10/2025
25-7000	9/9/2025	9/10/2025
25-7012	9/9/2025	9/10/2025
25-7125	9/12/2025	9/15/2025
25-7163	9/15/2025	9/16/2025
25-7166	9/15/2025	9/16/2025
25-7301	9/19/2025	9/19/2025
25-7370	9/22/2025	9/23/2025
25-7405	9/22/2025	9/23/2025
25-7415	9/23/2025	10/2/2025
25-7549	9/27/2025	9/29/2025

Request Number (continued)	Request Date	Closed Date
25-7599	9/29/2025	9/30/2025
25-7749	10/2/2025	10/2/2025
25-7791	10/3/2025	10/7/2025
25-7848	10/6/2025	10/7/2025
25-7858	10/7/2025	11/25/2025
25-7903	10/8/2025	10/8/2025
25-7963	10/9/2025	10/10/2025
25-7971	10/10/2025	10/10/2025
25-7991	10/10/2025	10/13/2025
25-8045	10/13/2025	10/13/2025
25-8038	10/13/2025	10/14/2025
25-8009	10/12/2025	10/13/2025
25-8129	10/15/2025	10/24/2025
25-8122	10/15/2025	10/16/2025
25-7885	10/7/2025	10/21/2025
25-8239	10/20/2025	10/21/2025
25-8268	10/20/2025	10/21/2025
25-8290	10/21/2025	10/22/2025
25-8308	10/22/2025	10/22/2025
25-8345	10/23/2025	10/23/2025
25-8349	10/23/2025	10/23/2025
25-8354	10/23/2025	10/23/2025
25-8500	10/28/2025	10/29/2025
25-8513	10/28/2025	10/29/2025
25-8569	10/30/2025	11/4/2025
25-8587	10/30/2025	11/4/2025
25-8682	11/3/2025	11/4/2025
25-8681	11/3/2025	11/4/2025
25-8655	11/3/2025	11/4/2025
25-8778	11/5/2025	11/6/2025
25-8804	11/6/2025	11/6/2025
25-8846	11/7/2025	11/7/2025
25-8885	11/8/2025	11/13/2025
25-8898	11/9/2025	11/10/2025
25-9024	11/12/2025	11/21/2025
25-9082	11/14/2025	11/14/2025

Request Number (continued)	Request Date	Closed Date
25-9102	11/14/2025	11/14/2025
25-9152	11/17/2025	11/17/2025
25-9182	11/18/2025	11/24/2025
25-9160	11/17/2025	11/17/2025
25-9161	11/17/2025	11/18/2025
25-9246	11/19/2025	11/20/2025
25-9267	11/20/2025	11/20/2025
25-9320	11/21/2025	11/24/2025
25-9333	11/22/2025	11/24/2025
25-9541	12/1/2025	12/2/2025
25-9556	12/2/2025	12/11/2025
25-9551	12/2/2025	12/3/2025
25-9580	12/2/2025	12/3/2025
25-9366	11/24/2025	12/4/2025
25-9623	12/3/2025	12/4/2025
25-9695	12/5/2025	12/5/2025
25-9634	12/3/2025	12/8/2025
25-9752	12/8/2025	12/16/2025
25-9770	12/8/2025	12/9/2025
25-9783	12/8/2025	12/9/2025
25-9826	12/9/2025	12/10/2025
25-9846	12/10/2025	12/11/2025
25-9867	12/10/2025	12/11/2025
25-9902	12/11/2025	12/12/2025
25-9930	12/12/2025	12/16/2025
25-9752	12/8/2025	12/16/2025
25-9925	12/12/2025	OPEN
25-10101	12/17/2025	12/18/2025
25-10266	12/22/2025	12/26/2025
25-10313	12/23/2025	12/26/2025
25-10327	12/24/2025	12/30/2025
25-10465	12/30/2025	12/31/2025
25-10481	12/30/2025	12/31/2025
25-10488	12/30/2025	12/31/2025
25-10490	12/30/2025	12/31/2025

ANNUAL COST

210.0102(a)(12) Total annual costs for the surveillance technology, including any specific personnel-related and other ongoing costs, and what source will fund the surveillance technology in the coming year.

San Diego's Smart Streetlight system includes two partner technologies: situational awareness video cameras and Automated License Plate Recognition (ALPR) cameras.

The annual service cost for the two integrated technologies is $2,012,500, based on a per-unit rate of $4,025.

Under the contract, all service fees are billed and paid in advance. On December 11, 2024, the City of San Diego paid the 2025 annual service fee.

Because not all 500 units were installed by the end of 2024, the vendor adjusted the fee to reflect the number of operational units, reducing the total from $2,012,500 to $1,449,602.08.

On December 11, 2024, a payment of $1,449,602.08 was authorized for calendar year 2025 contract obligations.

In May 2025, a payment of $4,000 was disbursed to Ubicquia to cover the cost of a damaged SSL unit resulting from a traffic collision.

In August 2025, a payment of $4,000 was disbursed to Ubicquia for a damaged SSL unit caused by a traffic collision.

In October 2025, a Smart Streetlight hub was mistakenly removed and disposed of as inoperative. This was done by a contractor at a construction site. SDPD put Ubicquia in contact with the contractor, and reimbursement was handled between those two entities.

All funding sources were from the City General Fund.

There are no personnel costs associated with this technology outside of normal operating parameters.

REQUESTED MODIFICATIONS TO THE USE POLICY

210.0102(a)(13) Any requested modifications to the Surveillance Use Policy and a detailed basis for the request.

At this time, no modifications to the Use Policy have been proposed.

San Diego Police Department Special Weapons and Tactics

SDPD

ONE TEAM. ONE MISSION.

San Diego Police Department

SWAT Unit Robots – First Look (Gen 1 & 2) and ICOR Mini Caliber

Department/Division: Police/Special Operations – Special Weapons and Tactics (SWAT) Unit

Related Policy/Procedure:

- DP 3.02 - Impound, Release, and Disposal of Property, Evidence, and Articles Missing Identification Marks

---

DESCRIPTION

The SDPD Special Weapons and Tactics (SWAT) team utilizes the ICOR robot and First Look (Gen 1 and 2) robots to help gather intelligence during rapidly evolving critical incidents.

The robots that are used by SDPD's SWAT Unit are all tracked remote-controlled cameras that can use both "white" light and infrared (IR) light to gain critical intelligence of an area that is deemed too dangerous to put a person or where a person may not physically fit. All of these robots send a signal from the camera on the robot to a monitor controlled by the SWAT operator. All of the robots have multiple cameras on them enabling the operator to see the environment from different angles.

In 2025, the SWAT Unit used the following robot makes and models during operations:

- ICOR Mini Caliber
- FirstLook (Gen 1)
- FirstLook (Gen 2)

While the essence of the robots are similar, there are a few capabilities each robot has that offers the SWAT Unit the ability to carry out its mission in the safest manner possible.

The ICOR Mini Caliber robot has a mechanical arm attached to it that allows the operator the ability to open closed doors and it has the ability to climb and descend stairs. The ICOR Mini Caliber robot is the heaviest of the robots, weighing approximately 64 pounds. The ICOR Mini Caliber has the ability to listen to its surroundings but does not have the ability to record any data. The ICOR robot was used 33 times during 2025.

One such deployment was the ICOR robot placing the under the door camera under a hotel door in order to confirm the suspect was in the hotel room.

The FirstLook (Gen 1) and (Gen 2) are lightweight robots that can be hand delivered or thrown into areas that may be difficult to access otherwise. The FirstLook robots have a "mesh network" which enables them to relay a signal from one robot to another and back to the controller in order to extend the range of the robots. The FLIR FirstLook (Gen 1) robot is equipped with a microphone and can hear live audio and relay that sound back to the operator's controller. The FLIR FirstLook (Gen 1) robot does not record or have the ability to record audio. The FirstLook (Gen 2) robot is able to record and listen to the environment via microphones and the operator is able to speak through the robot via speakers. The FirstLook (Gen 1 and Gen 2) robots were used approximately 23 times during 2025.

SHARING OF DATA

No data from these robots was shared with third parties or outside agencies.

LOCATION

The robots are used by the SWAT unit exclusively personnel and housed in SDPD facilities when not in use. The SWAT unit robots are deployed wherever the SWAT unit is called to in an attempt to bring a peaceful resolution to a critical incident. The robots are not attached to any objects.

UPDATES, UPGRADES, AND CONFIGURATION CHANGES

Repairs have been made to the ICOR robot, but there were no upgrades or changes to the operation of the robot. No updates, upgrades, or configuration changes have occurred in 2025 with these technologies.

DEPLOYMENT LOCATION

The SWAT unit utilizes the robots only when called upon by an incident commander. These robots were used in a variety of divisions across the city.

The San Diego Police Department SWAT Unit is a reactive unit that is called upon by the department to help bring a peaceful resolution to a critical incident. The SWAT Unit robots were deployed 36 times throughout all police service areas in support of high-risk tactical operations, search warrants, or other SWAT support functions.

POLICE SERVICE AREA	DEPLOYMENT Icor Mini	DEPLOYMENT First Look 1 or 2
NORTHERN DIVISION (100S)	2	1
NORTHEASTERN DIVISION (200S)	3	3
EASTERN DIVISION (300S)	3	2
SOUTHEASTERN DIVISION (400s)	7	5
CENTRAL DIVISION (500s)	3	1
WESTERN DIVISION (600s)	1	0
SOUTHERN DIVISION (700s)	5	2
MID-CITY DIVISION (800s)	5	5
NORTHWESTERN DIVISION (900s)	0	0
OUT OF CITY (BEAT 999)	3	3

COMMUNITY COMPLAINTS OR CONCERNS

The Department is committed to protecting civil rights and liberties of our citizens as presented to the City Council prior to approval of this technology. The Department has not received any complaints or concerns about this surveillance technology or received any reports of disproportionate impacts. The Use Policy continues to protect civil rights and civil liberties.

AUDITS OR INVESTIGATIONS

In response to the Privacy Advisory Board's (PAB) Memorandum addressed to San Diego City Council President LaCava and Members of the San Diego City Council on April 17, 2025, which provided a request for more rigorous auditing processes, the SDPD's Research, Analysis, and Planning Division published Department Order (OR) 25-13 on April 25, 2025. This order requires the managing unit (the managing unit is the person(s) recognized as the subject matter expert (SME) for the Transparent and Responsible Use of Surveillance Technology ordinance reporting or who controls the equipment) to prepare for the required Annual Report each year. The OR requires that the SMEs conduct quarterly audits of the equipment they are in charge of, including compiling and tracking information and data listed in SDMC 210.0102(a). On July 15, 2025, an additional Department Order, DO 25-23, was published. This DO requires Department members using any technology or database to enter a reference code/ID or justification for use of the technology or database with either a relevant full eight-digit case number, a full 11-digit event number, or other unique identification code. It requires that users no longer use nonspecific phrases or references and enhances the ability to audit the system.

In accordance with OR 25-13, and as an addition to the required quarterly audits by the managing unit, an independent audit was conducted by the Research, Analysis, and Planning Division (RAP)– Inspection and Control Unit. The audits were in addition to the quarterly audits required by the managing unit in OR 25-13. These audits targeted confirmation of the proper use of the technology, as stated in the Use Policy.

These technologies were audited on 36 different case numbers, event numbers, or use statistics to verify the proper use of the technology. No unauthorized uses of the technology were located during the audit conducted by RAP.

These technologies are contained in a secured facility and are only accessed by SWAT personnel.

Any training issues or unintended input errors with this technology were identified and corrected. Continued errors or training issues will result in the user being suspended from the technology until they can be retrained on the technology.

Any substantial non-compliance or intentional misuse will be forwarded to the command or the Internal Affairs Unit for investigation and the subject may have their access permanently removed from the technology.

There were no reported violations of the Surveillance Use Policy or SDPD Policy or Procedure regarding this technology.

DATA BREACH OR UNAUTHORIZED ACCESS

The City of San Diego's Department of Information Technology and SDPD Information Technology Unit has identified no data breaches or unauthorized access to the data collected by the surveillance technology.

DATA BREACH DETECTION

The City's Department of Information Technology oversees the IT governance process and works with SDPD's Department of IT regarding project execution and risk assessment as well as selecting and approving technology solutions. Cyber security and technology risks are also

assessed by the Department of IT. For additional details related to IT governance processes, refer to the information at the following link:

https://www.sandiego.gov/sites/default/files/fy23-fy27-it-strategic-plan-sd.pdf

INFORMATION AND STATISTICS

The SWAT Unit does not produce, collect or share crime statistics and there are no direct relational crime statistics associated with or produced by the use of this technology.

These technologies allow SDPD SWAT personnel to gain situational awareness of 90% of any structures or areas they are operating in. They assist in identifying any hazards or safety issues for suspect and officer safety. They also assist in de-escalation by way of being able to see suspect actions and to plan accordingly to evaluate responses ahead of suspect contact, when possible.

Should the public want to access crime statistics for the City of San Diego, they can visit the City's *Crime Statistics & Crime Mapping* webpage: Crime Statistics & Crime Mapping | City of San Diego Official Website. The City's neighborhood crime summary dashboard is available at: San Diego Neighborhood Crime Dashboard (arcgis.com). A tab on this dashboard, Crime Data Explorer, allows the user to query crimes specific to a City neighborhood.

Additionally, crime data is also available on the City's Open Data Portal: Datasets - City of San Diego Open Data Portal. This crime data can be downloaded into usable files; also available on this site are dictionaries to help navigate the different data sets.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

The information produced in response to these requests can be viewed on the City of San Diego's CPRA request portal: https://sandiego.nextrequest.com/

REQUEST NUMBER	REQUEST DATE	CLOSED DATE
25-7858	10/07/2025	11/02/2025

ANNUAL COST

In 2025, the two technologies utilized the following budget:

Teledyne FLIR and ICOR robots have a budget of $12,100 a year, which is funded by the General Fund.

One of ICOR robots was shipped back to the manufacturer for repair. This repair cost is $711.03.

REQUESTED MODIFICATIONS TO THE USE POLICY

There were no requested modifications to these technologies' use policy.

San Diego Police Department

Swift Under Door Camera

Department/Division: Police - Special Weapons and Tactics (SWAT) Unit

Related Policy/Procedure:

- 3.02- Impound, Release, and Disposal of Property, Evidence, and Articles Missing Identification Marks

---

DESCRIPTION

The SWAT team utilizes the Under the Door camera to help gather intelligence during rapidly evolving critical incidents. This technology was used in an effort to minimize risk to officers and citizens as well as help de-escalate critical incidents often involving armed or otherwise dangerous suspects. Through the use of this camera, this technology provides a video image of a space that cannot be seen with the human eye or is too dangerous to place a human. The Under the Door camera was deployed twice in 2025.

SHARING OF DATA

Any information that was gathered from this technology was not recorded. As such, no data was shared with any non-City entities.

LOCATION

This technology is a mobile tool used to gain situational awareness in an area that is deemed either dangerous to go into or not able to fit a human being.

UPDATES, UPGRADES, AND CONFIGURATION CHANGES

There have been no updates, upgrades, or configuration changes that expanded or reduced the surveillance technology capabilities.

DEPLOYMENT LOCATION

This technology was deployed twice in 2025. Once in the Southeastern Division police service area and once in the Eastern police service area.

POLICE SERVICE AREA	DEPLOYMENT Under Door Camera
EASTERN DIVISION (500s)	1
OUT OF CITY (BEAT 999)	1
TOTAL	**2**

COMMUNITY COMPLAINTS OR CONCERNS

The SDPD is committed to protecting the civil rights and liberties of our citizens as presented to the City Council for approval of this technology. The SDPD has not received any complaints or concerns about this surveillance technology or received any reports of disproportionate impacts. The Use Policy continues to protect civil rights and civil liberties.

AUDITS OR INVESTIGATIONS

In response to the Privacy Advisory Board's (PAB) Memorandum addressed to San Diego City Council President LaCava and Members of the San Diego City Council on April 17, 2025, which provided a request for more rigorous auditing processes, the SDPD's Research, Analysis, and Planning Division published Department Order (OR) 25-13 on April 25, 2025. This order requires the managing unit (the managing unit is the person(s) recognized as the subject matter expert (SME) for the Transparent and Responsible Use of Surveillance Technology ordinance reporting or who controls the equipment) to prepare for the required Annual Report each year. The OR requires that the SMEs conduct quarterly audits of the equipment they are in charge of, including compiling and tracking information and data listed in SDMC 210.0102(a). On July 15, 2025, an additional Department Order, DO 25-23, was published. This DO requires Department members using any technology or database to enter a reference code/ID or justification for use of the technology or database with either a relevant full eight-digit case number, a full 11-digit event number, or other unique identification code. It requires that users no longer use nonspecific phrases or references and enhances the ability to audit the system.

In accordance with OR 25-13, and as an addition to the required quarterly audits by the managing unit, an independent audit was conducted by the Research, Analysis, and Planning Division (RAP)– Inspection and Control Unit. The audits were in addition to the quarterly audits required by the managing unit in OR 25-13. These audits targeted confirmation of the proper use of the technology, as stated in the Use Policy.

This technology was used twice during 2025 and was audited two times on different case number, event number, or use statistics to verify the proper use of the technology. No unauthorized uses of the technology were located during the audit conducted by RAP.

This technology is contained in a secured facility and are only accessed by SWAT personnel.

Any training issues or unintended input errors with this technology were identified and corrected. Continued errors or training issues will result in the user being suspended from the technology until they can be retrained on the technology.

Any substantial non-compliance or intentional misuse will be forwarded to the command or the Internal Affairs Unit for investigation and the subject may have their access permanently removed from the technology.

There were no reported violations of the Surveillance Use Policy or SDPD Policy or Procedure regarding this technology.

DATA BREACH OR UNAUTHORIZED ACCESS

The City of San Diego's Department of Information Technology and SDPD Information Technology Unit has identified no data breaches or unauthorized access to the data collected by the surveillance technology.

DATA BREACH DETECTION

The City's Department of Information Technology oversees the IT governance process and works with SDPD's Department of IT regarding project execution and risk assessment as well as selecting and approving technology solutions. Cyber security and technology risks are also assessed by the Department of IT. For additional details related to IT governance processes, refer to the information at the following link:

https://www.sandiego.gov/sites/default/files/fy23-fy27-it-strategic-plan-sd.pdf

INFORMATION AND STATISTICS

The SWAT Unit does not produce, collect or share crime statistics and there are no direct relational crime statistics associated with or produced by the use of this technology.

This technology allows SDPD SWAT personnel to gain situational awareness in any structures or areas they are operating in. They assist in identifying any hazards or safety issues for suspect and officer safety. They also assist in de-escalation by way of being able to see suspect actions and to plan accordingly to evaluate responses ahead of suspect contact, when possible. This technology was deployed twice in 2025.

One of those deployments allowed the SDPD SWAT units to check under a hotel door during a mission. The camera identified the suspect.

Should the public want to access crime statistics for the City of San Diego, they can visit the City's *Crime Statistics & Crime Mapping* webpage: Crime Statistics & Crime Mapping | City of San Diego Official Website. The City's neighborhood crime summary dashboard is available at: San Diego Neighborhood Crime Dashboard (arcgis.com). A tab on this dashboard, Crime Data Explorer, allows the user to query crimes specific to a City neighborhood.

Additionally, crime data is also available on the City's Open Data Portal: Datasets - City of San Diego Open Data Portal. This crime data can be downloaded into usable files; also available on this site are dictionaries to help navigate the different data sets.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

The information produced in response to these requests can be viewed on the City of San Diego's CPRA request portal: https://sandiego.nextrequest.com/

REQUEST NUMBER	REQUEST DATE	CLOSED DATE
25-7858	10/07/2025	11/02/2025

ANNUAL COST

In 2025, SDPD did not expend any funds for this technology and does not have any projected costs in 2026 regarding this technology.

REQUESTED MODIFICATIONS TO THE USE POLICY

There were no requested modifications to this technology's Use Policy.

San Diego Police Department Tracking Equipment

SDPD

ONE TEAM. ONE MISSION.

San Diego Police Department

Code5Group GPS-Integrated Bike

Department/Division: Police -Northern Division and Neighborhood Policing Division

Related Policy/Procedure: None

DESCRIPTION

Global Positioning System (GPS) integrated bicycles allow officers, through a phone application or desktop computer, to place and remotely monitor GPS-integrated bicycles. Commonly referred to as "bait bikes," these bikes are secured to a bike rack or other immovable object. GPS tracking begins only after a bicycle is stolen. Officers are notified of movement and can track the bicycle's location in real-time. The technology allows SDPD to combat bicycle thefts without the need for officers in static positions while giving the ability to track/apprehend the equipment using the GPS. The software and application allow virtual perimeters to be created around GPS integrated bicycles and enable alert notifications. Officers use the vendor application to create virtual perimeters, live track a GPS integrated bicycle, and collect location data for reports.

GPS tracking devices allow "bait bicycle" operations. These operations are very effective in apprehending stolen bikes in high theft areas of San Diego. The operation and access to the GPS software is limited to official law enforcement purposes only. Officers operating the GPS devices and software are trained and given authorization from supervisors prior to use. GPS integrated bicycles allow officers to place, get notifications of movement, track in real time, and apprehend.

The Bait Bicycle technology was used ten (10) times in 2025. There were five (5) arrests made using this technology, which were forwarded to the DA's Office for prosecution.

SHARING OF DATA

In 2025, data, in the form of written reports concerning the initial location of the bike and its recovery location, was shared with the District Attorney's Office. The District Attorney's office prosecutes arrests regarding this technology due to the cost of the bicycle being valued at a minimum of $1,000. The testimony is also shared with criminal defendants and their attorneys through the criminal discovery process. No data was shared outside the criminal prosecutorial chain.

Five (5) cases were sent to the District Attorney's Office for prosecution.

LOCATION

The department currently has three GPS-integrated bicycles. The bicycles are stored at two different divisions. Bikes are rotated between the two locations as needed for operational use or repair. The integrated GPS hardware is secreted within the bicycle apparatus.

UPDATES, UPGRADES, AND CONFIGURATION CHANGES

There have been no updates, upgrades, or configuration changes that expanded or reduced the surveillance technology capabilities.

DEPLOYMENT LOCATION

The department's bait bikes are deployed in areas known for high crime and theft. The surveillance technology operates in the San Diego Police Northern Division area (100 Service Area) and Central Division area (500 Service Area).

Police Service Area	Deployment	Arrests
NORTHERN DIVISION (100S)	3	0
CENTRAL DIVISION (500s)	7	5

COMMUNITY COMPLAINTS OR CONCERNS

The Department is committed to protecting civil rights and liberties of our citizens as presented to the City Council prior to approval of this technology. The Department has not received any complaints or concerns about this surveillance technology.

AUDITS OR INVESTIGATIONS

In response to the Privacy Advisory Board's (PAB) Memorandum addressed to San Diego City Council President LaCava and Members of the San Diego City Council on April 17, 2025, which provided a request for more rigorous auditing processes, the SDPD's Research, Analysis, and Planning Division published Department Order (OR) 25-13 on April 25, 2025. This order requires the managing unit (the managing unit is the person(s) recognized as the subject matter expert (SME) for the Transparent and Responsible Use of Surveillance Technology ordinance reporting or who controls the equipment) to prepare for the required Annual Report each year. The OR requires that the SMEs conduct quarterly audits of the equipment they are in charge of, including compiling and tracking information and data listed in SDMC 210.0102(a). On July 15, 2025, an additional Department Order, DO 25-23, was published. This DO requires Department members using any technology or database to enter a reference code/ID or justification for use of the technology or database with either a relevant full eight-digit case number, a full 11-digit event number, or other unique identification code. It requires that users no longer use nonspecific phrases or references and enhances the ability to audit the system.

In accordance with OR 25-13, and as an addition to the required quarterly audits by the managing unit, an independent audit was conducted by the Research, Analysis, and Planning Division (RAP)– Inspection and Control Unit. The audits were in addition to the quarterly audits required by the managing unit in OR 25-13. These audits targeted confirmation of the proper use of the technology, as stated in the Use Policy.

This technology was audited on all ten (10) different case numbers, event numbers, or use statistics to verify the proper use of the technology. All ten uses were documented placements of the technology. No unauthorized uses of the technology were located during the audit conducted by RAP.

Any training issues or unintended input errors with this technology were identified and corrected. Continued errors or training issues will result in the user being suspended from the technology until they can be retrained on the technology.

Any substantial non-compliance or intentional misuse will be forwarded to the command or the Internal Affairs Unit for investigation and the subject may have their access permanently removed from the technology.

There were no reported violations of the Surveillance Use Policy or SDPD Policy or Procedure regarding this technology.

DATA BREACH OR UNAUTHORIZED ACCESS

The City of San Diego's Department of Information Technology and SDPD Information Technology Unit has identified no data breaches or unauthorized access to the data collected by the surveillance technology.

DATA BREACH DETECTION

The City's Department of Information Technology oversees the IT governance process and works with SDPD's Department of IT regarding project execution and risk assessment as well as selecting and approving technology solutions. Cyber security and technology risks are also assessed by the Department of IT. For additional details related to IT governance processes, refer to the information at the following link:

https://www.sandiego.gov/sites/default/files/fy23-fy27-it-strategic-plan-sd.pdf

INFORMATION AND STATISTICS

There are no direct relational crime statistics associated with or produced by the use of this technology.

Should the public want to access crime statistics for the City of San Diego, they can visit the City's *Crime Statistics & Crime Mapping* webpage: Crime Statistics & Crime Mapping | City of San Diego Official Website. The City's neighborhood crime summary dashboard is available at: San Diego Neighborhood Crime Dashboard (arcgis.com). A tab on this dashboard, Crime Data Explorer, allows the user to query crimes specific to a City neighborhood.

Additionally, crime data is also available on the City's Open Data Portal: Datasets - City of San Diego Open Data Portal. This crime data can be downloaded into usable files; also available on this site are dictionaries to help navigate the different data sets.

Of the ten (10) deployments of this technology, there were five (5) arrests with cases submitted to the DA's Office for prosecution.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

The information produced in response to these requests can be viewed on the City of San Diego's CPRA request portal: https://sandiego.nextrequest.com/

REQUEST NUMBER	REQUEST DATE	CLOSED DATE
25-7858	10/07/2025	11/02/2025

ANNUAL COST

The annual fiscal cost of the software comes from the Information Technology budget. For FY 2025 the budget was $2,400. The FY 2026 budget is $2,904. The funds for services and bike repairs are paid through General Fund. This will continue in 2027.

REQUESTED MODIFICATIONS TO THE USE POLICY

There are no requested modifications to this technology's Use Policy.

San Diego Police Department

Vehicle and Object Trackers

Department/Division: Police - Investigations II - Robbery

Related Policy/Procedure:

- DP 3.02 / Investigative Operations Manuals

DESCRIPTION

These technologies collect location data by using GPS and cellular towers. As the tracker moves it collects the GPS coordinates and the speed of the device.

The Department utilizes vehicle tracking devices to track suspect vehicles involved in ongoing criminal investigations, locate wanted suspects, or locate stolen property.

The Department utilizes object tracking devices to track suspects and locate stolen property. These trackers were not utilized in the 2025 calendar year.

SHARING OF DATA

Sharing of data is at the discretion of the detective handling the investigation.

Location data may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes, which includes criminal investigations and prosecution as allowed by law. The data was not used in immigration enforcement.

LOCATION

The specific locations where this technology was utilized is being withheld as it could undermine the legitimate security interests of the city.

UPDATES, UPGRADES, AND CONFIGURATION CHANGES

There have been no upgrades or configuration changes to this technology during the 2025.

DEPLOYMENT LOCATION

The vehicle trackers were deployed in all SDPD service areas.

COMMUNITY COMPLAINTS OR CONCERNS

The Department is committed to protecting civil rights and liberties of all citizens as presented to the City Council prior to the approval of this technology. The department did not receive any complaints or concerns regarding this surveillance technology or receive any reports of disproportionate impacts. The Use Policy protected civil rights and liberties.

These devices are used to track specific targets, not general groups. The devices require a warrant to be utilized or in certain circumstances the devices can be utilized without a warrant on subjects with 4th Amendment waivers.

AUDITS OR INVESTIGATIONS

In response to the Privacy Advisory Board's (PAB) Memorandum addressed to San Diego City Council President LaCava and Members of the San Diego City Council on April 17, 2025, which provided a request for more rigorous auditing processes, the SDPD's Research, Analysis, and Planning Division published Department Order (OR) 25-13 on April 25, 2025. This order requires the managing unit (the managing unit is the person(s) recognized as the subject matter expert (SME) for the Transparent and Responsible Use of Surveillance Technology ordinance reporting or who controls the equipment) to prepare for the required Annual Report each year. The OR requires that the SMEs conduct quarterly audits of the equipment they are in charge of, including compiling and tracking information and data listed in SDMC 210.0102(a). On July 15, 2025, an additional Department Order, DO 25-23, was published. This DO requires Department members using any technology or database to enter a reference code/ID or justification for use of the technology or database with either a relevant full eight-digit case number, a full 11-digit event number, or other unique identification code. It requires that users no longer use nonspecific phrases or references and enhances the ability to audit the system.

In accordance with OR 25-13, and as an addition to the required quarterly audits by the managing unit, an independent audit was conducted by the Research, Analysis, and Planning Division (RAP)– Inspection and Control Unit. The audits were in addition to the quarterly audits required by the managing unit in OR 25-13. These audits targeted confirmation of the proper use of the technology, as stated in the Use Policy.

This technology was not utilized in 2025. As such, no audit was completed for these technologies. This technology is secured by physical security measures and requires legal authority, such as a search warrant or 4th Amendment waiver, and a three-person authorization from the managing unit technical officer, detective sergeant, and lieutenant before use. No unauthorized uses of the technology were located during the audit conducted by RAP.

Any training issues or unintended input errors with this technology were identified and corrected. Continued errors or training issues will result in the user being suspended from the technology until they can be retrained on the technology.

Any substantial non-compliance or intentional misuse will be forwarded to the command or the Internal Affairs Unit for investigation and the subject may have their access permanently removed from the technology.

There were no reported violations of the Surveillance Use Policy or SDPD Policy or Procedure regarding this technology.

DATA BREACH OR UNAUTHORIZED ACCESS

The City of San Diego's Department of Information Technology and SDPD Information Technology Unit has identified no data breaches or unauthorized access to the data collected by the surveillance technology.

DATA BREACH DETECTION

The City's Department of Information Technology oversees the IT governance process and works with SDPD's Department of IT regarding project execution and risk assessment as well

as selecting and approving technology solutions. Cyber security and technology risks are also assessed by the Department of IT. For additional details related to IT governance processes, refer to the information at the following link:

https://www.sandiego.gov/sites/default/files/fy23-fy27-it-strategic-plan-sd.pdf

INFORMATION AND STATISTICS

There are no direct relational crime statistics associated with or produced by the use of this technology.

Should the public want to access crime statistics for the City of San Diego, they can visit the City's *Crime Statistics & Crime Mapping* webpage: Crime Statistics & Crime Mapping | City of San Diego Official Website. The City's neighborhood crime summary dashboard is available at: San Diego Neighborhood Crime Dashboard (arcgis.com). A tab on this dashboard, Crime Data Explorer, allows the user to query crimes specific to a City neighborhood.

Additionally, crime data is also available on the City's Open Data Portal: Datasets - City of San Diego Open Data Portal. This crime data can be downloaded into usable files; also available on this site are dictionaries to help navigate the different data sets.

CALIFORNIA PUBLIC RECORDS ACT REQUEST

The information produced in response to these requests can be viewed on the City of San Diego's CPRA request portal: https://sandiego.nextrequest.com/

REQUEST NUMBER	REQUEST DATE	CLOSED DATE
25-7858	10/07/2025	11/02/2025

ANNUAL COST

The cost for the service is $7,020.00 a year for the vehicle trackers.

The cost for the service is $1440.00 a year for the object trackers.

Both items are from the General Fund and this will continue in FY 2027.

REQUESTED MODIFICATIONS TO THE USE POLICY

There are no requested modifications to these technologies' Use Policies.

Conclusion

SDPD
ONE TEAM. ONE MISSION.

The technologies covered in this report support public safety by enhancing situational awareness, enabling the safe resolution of critical incidents, and assisting in lawful criminal investigations. Their approved and proposed uses include safeguards designed to protect civil rights and civil liberties, and no effective alternative has been identified that would deliver comparable public safety benefits at a lower financial cost or with less impact on civil rights or civil liberties.

At the same time, the Department remains committed to transparency and welcomes feedback regarding the use of these critical technologies. By submitting this report, the SDPD has fulfilled its annual reporting obligations under the Municipal Code and looks forward to continued collaboration with the Privacy Advisory Board, community stakeholders, and the City Council to ensure the responsible and transparent use of surveillance technology.