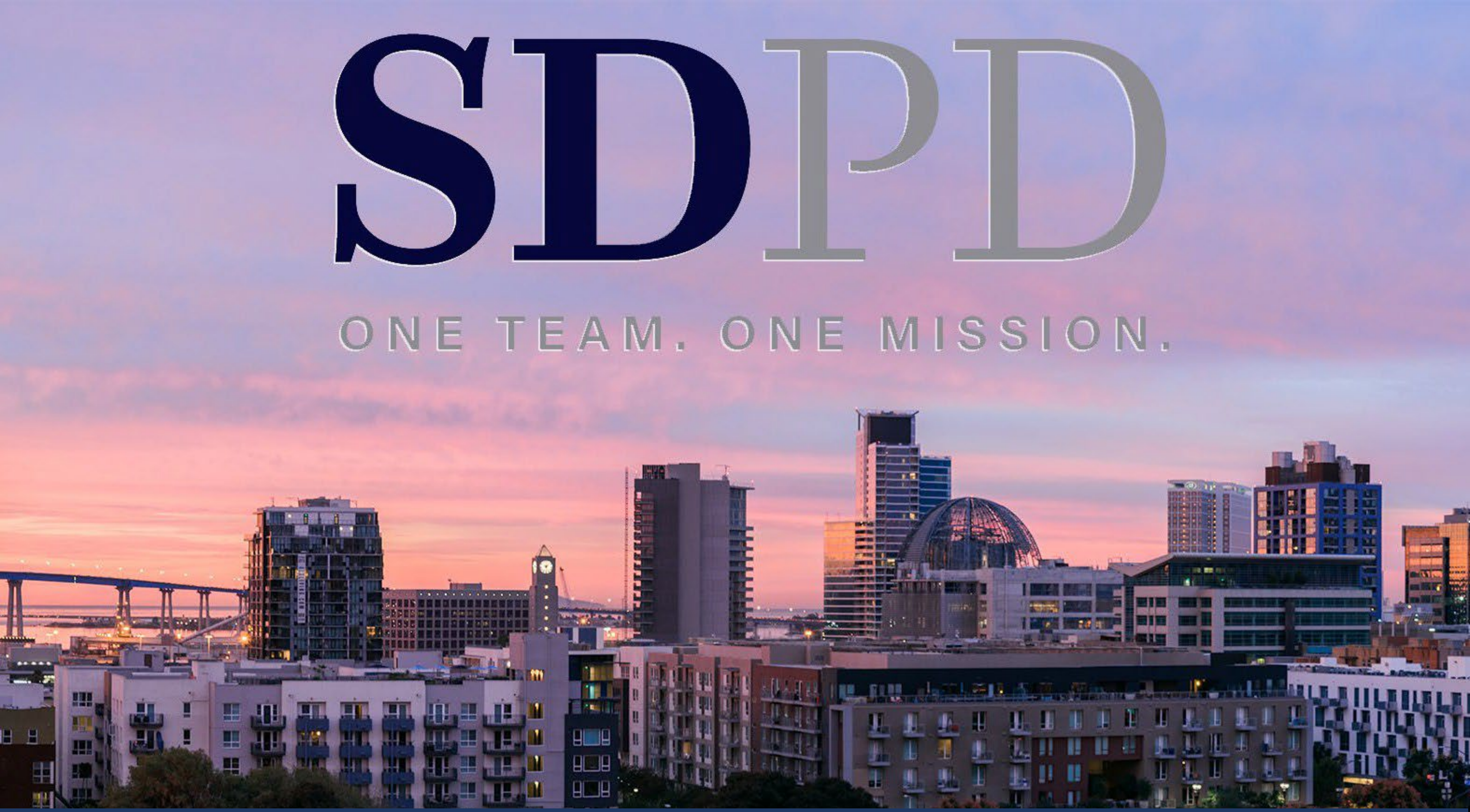


SDPD

ONE TEAM. ONE MISSION.

Annual Surveillance Report

San Diego Police Department

2024

Introduction

Executive Summary

Introduction

The San Diego Police Department (SDPD) is committed to maintaining public safety by providing the highest quality police services to the communities we serve. Given today's technological advancements with surveillance equipment, the SDPD understands the need to provide the community with a partnership that allows our community stakeholders an active voice in the policing of their communities. In addition to maintaining the highest levels of public safety, the SDPD is committed to transparency, public trust, community partnerships, and compliance with the law. As such, the Department has authored the following 2024 Annual Surveillance Report in accordance with annual reporting requirements codified in the San Diego Municipal Code.

The surveillance equipment listed in this annual report are essential and may be required from time to time to aid in de-escalating intense situations, crimes against persons and property, enhance responses to critical incidents, minimize public threats, safeguard the lives of community members, and or resolving volatile conditions and critical incidents safely, along with providing valuable criminal investigative tools for actionable evidence available after these crimes have been committed. These authorized technologies safeguard civil liberties and civil rights and are used by the SDPD to protect the community members, visitors, assets, and resources of the City of San Diego.

Definitions

Annual Surveillance Report

> Annual Surveillance Report means a written report concerning specific surveillance technology that includes all of the following elements:
>
> (1) A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the surveillance technology.
>
> (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.
>
> (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.
>
> (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.

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

(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.

(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.

(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.

(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.

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

(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 close date for each of these California Public Records Act requests.

(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.

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

Surveillance Use Policy:

Surveillance Use Policy means a publicly released and legally enforceable policy for the use of specific *surveillance technology* that includes all of the following elements:

(1) Purpose: The specific purposes that the *surveillance technology* is intended to advance.

(2) Use: The specific uses that are authorized and the rules and processes required prior to the use, 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*.

(3) Data Collection: The information that can be collected, captured, recorded, intercepted, or retained by the *surveillance technology*, data that may be inadvertently collected during the authorized uses of the *surveillance technology* and what measures will be taken to minimize and delete the data, and any data sources the *surveillance technology* will rely upon, as applicable, 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*.

(4) Data Access: The job classification of *individuals* who can access or use the collected information, and the rules and processes required prior to access or use of the information, 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*.

(5) Data Protection: The safeguards that protect information from unauthorized access, including system logging, encryption, and access control mechanisms, 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*.

(6) Data Retention: The time period, if any, for which information collected by the *surveillance technology* will be routinely retained, the reason the retention period is appropriate to further the purposes, the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period.

(7) Public Access: A description of how collected information can be accessed or used by members of the public, including criminal defendants.

(8) Third Party Data Sharing: If and how information obtained from the *surveillance technology* can be accessed or used, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information.

(9) Training: The training required for any individual authorized to use the *surveillance technology* or to access information collected by the *surveillance technology*.

(10) Auditing and Oversight: The procedures used to ensure that the *Surveillance Use Policy* is followed, including identification of internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the *surveillance technology* and access to information collected by the *surveillance technology*, technical measures to monitor for misuse, identification of any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy.

(11) Maintenance: The procedures used to ensure that the security and integrity of the *surveillance technology* and collected information will be maintained.

Surveillance Technology:

Surveillance technology means any software (for example, scripts, code, or Application Programming Interfaces), electronic device, system utilizing an electronic device, or similar device, which is used, designed, or primarily intended to observe, collect, retain, analyze, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any *individual* or group. It also includes the product (for example, audiovisual recording, data, analysis, or report) of the *surveillance technology*. Examples of *surveillance technology* include the following: cell site simulators (Stingrays); automatic license plate readers; gunshot detectors (ShotSpotter); drone-mounted data collection; *facial recognition technology*; thermal imaging systems; body-worn cameras; social media analytics software; gait analysis software; and video cameras that record audio or video and transmit or can be remotely accessed. It also includes software designed to monitor social media services or forecast criminal activity or criminality, and biometric identification hardware or software.

Crime Statistics Summary

In 2024, the SDPD was responsible for patrolling 372.4 square miles, protecting 1.39 million residents, and receiving approximately 1.2 million calls from the community regarding crimes in progress, collisions, life-threatening situations, and a wide range of other public safety concerns. Of those calls for service, the SDPD responded to over 400,000 events. The SDPD documented over 62,000 crime cases affecting the various communities of San Diego and visitors to our great city. The SDPD made the community safer by arresting over 31,000 persons, including those who victimized our most vulnerable community members. The volume of all this work was completed with only 1870 officers, thus making these technologies vital to the overall mission of the SDPD.

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 provide 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 between crewmembers), and imagery produced from the helicopter-mounted forward-looking infrared (FLIR) sensor during police-related incidents. The FLIR 380 HDc 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. 436 impounds of videos were made in 2024. Of those videos, approximately 240 videos were uploaded to Evidence.com for release to investigators or prosecutorial agencies.

ASU flew 2695 hours in 2024, 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 technology has the ability to save, track, analyze or capture data, which includes location of use, duration of use, or configuration of use.

SHARING OF DATA

Data recorded to the Avalex DVR via the FLIR 380 HDc 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 436 impounds of videos, 59 ASU videos were shared with outside law enforcement agencies during 2024. 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	5
California Highway Patrol (CHP)	13
El Cajon Police Department	6
La Mesa Police Department	4
National City Police Department	4
Riverside County Sherrif's Office	1
San Diego County District Attorney's Office	14
San Diego County Sherif's Office	8
DEA/NTF	1
United States Marine Corps	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 between crewmembers), and imagery produced from the helicopter-mounted forward-looking infrared (FLIR) sensor during police-related incidents. The FLIR 380 HDc 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 380 HDc 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 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

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

DATA BREACH OR UNAUTHORIZED ACCESS

The Department is not aware of data breaches or unauthorized access to the data collected by this 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, 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. 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.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

There were two (2) California Public Records Act requests referencing these technologies in 2024.

Requested Number	Requested Date	Closed Date
24-1779	03/11/2024	03/21/2024
24-2391	04/04/2024	04/11/2024

ANNUAL COST

All four FLIR 380 HDc sensors were purchased with federal grant money. All four are maintained with a Service Maintenance Agreement (SMA) through the manufacturer, Teledyne FLIR, and paid by the department’s general funds. The annual cost is $44,000.00 per year, per unit.

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.

San Diego Police Department

Unmanned Aerial Systems (UAS)

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

Unmanned Aircraft Systems (UAS), also known as a “drone” is a small aircraft under 55 pounds, operated without the possibility of direct human intervention from within or on the aircraft. The UAS was used to support first responders during critical incidents, to support investigations, and to provide enhanced security overwatch and anti-terrorist efforts during Special Events and large gatherings. The San Diego Police Department (SDPD) operated and used the following UAS models: UAS 01-DJI Phantom 4, DJI Matrice, Brinc Lemur, Shield Al Nova, DJI Mavic, Parrot Anafi, Acecore Zoe, Hoverfly, DJI Avata, Teledyne Flir Black Hornet, and FotoKite Sigma. 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.

UAS Technology and the Dejero DTS were utilized for the following mission types and objectives in 2024:

- Support SWAT Unit during incidents involving a barricaded suspect believed to be armed.
- Support SWAT during a high-risk warrant service.
- Searches for at-risk missing adult. (UAS only)
- Searches for at-risk missing juvenile. (UAS only)
- Aerial Overwatch at mass gathering special events to detect terrorism and criminal activity.
- Searches for fleeing felony suspect believed to be armed. (UAS only)
- Search for a felony child molest suspect. (UAS only)
- Capture video and photographic evidence of major crime scenes. (UAS only)

- Observe civil demonstrations to provide situational updates to incident commanders.
- Remotely inspect suspicious packages believed to be improvised explosive devices.
- Support Secret Service with Dignitary Protection details of Federal Government employees.
- Searches for a missing driver of a vehicle collision believed to be injured. (UAS only)
- Search rooftops for a suspect's discarded firearm to find evidence and support public safety. (UAS only)
- Support City Emergency Operations Center during flood response efforts to provide status on obstructed waterways and storm channels.
- Support Cal-Fire with a hazardous building inspection during a lithium battery building fire. (UAS only)
- Support negotiation efforts during an incident involving a suicidal person threatening to jump off a building.

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 2024, 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.

During one UAS Operation in 2024, video and photography was taken and retained but it was not captured as law enforcement related evidence to a crime. The digital media was taken and shared in support of Disaster Response efforts.

- May 20, 2024 – The San Diego Fire Department and Cal-Fire requested UAS Unit to assist with the interior inspection of a lithium battery storage facility that had caught on fire to collect data in structural integrity and the status of the fire. These videos and photos were shared with the Cal-Fire incident command.

Data is not collected on the DTS technology. This equipment is only used to transmit a live video feed from one source to another location. No data is recorded on this equipment and therefore there is no sharing of data.

LOCATION

For the majority of the 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.

The Dejero DTS is deployed with the SDPD UAS Unit which are primarily deployed citywide. SDPD UAS may also be deployed out of city limits and out of county if requested by an outside agency or if requested by an authorized SDPD unit who is responsible for a law enforcement operation beyond city limits. A primary example of this is when the UAS Unit is requested to collect aerial evidence photos for the SDPD Homicide Unit that is responsible to conduct the investigation when the San Diego Sheriff's department has an Officer Involved shooting.

To use the Dejero DTS it must be connected to a "video source" like a video camera or the ground controller display of an Unmanned Aircraft System (UAS). The Dejero DTS, specifically the Engo, takes the live video feed from the "video source" and transmits it via cellular signal to the Waypoint. The Waypoint is connected to the Cuepoint that creates an internet access point. SDPD personnel, who have access credentials can then access this live video via the internet.

UPDATES, UPGRADES, AND CONFIGURATION CHANGES

There have been no updates, upgrades, or configuration changes in the UAS or Dejero DTS as described in the ordinance.

DEPLOYMENT LOCATION

UAS and Dejero DTS are utilized throughout San Diego County. Our primary mission is to provide live video feed UAS assets for the San Diego Police Department.

UAS Technology was deployed to 102 incidents for SDPD. UAS camera technology was utilized for 98 of these 102 incidents. Of the 98 incidents that camera technology was used, at 61 of the incidents evidence was collected in either video or photographic form, while at the other 37 incidents the UAS camera technology was used for observation only and did not record any evidence.

UAS technology was physically flown for 93 of these 102 incidents, while UAS camera systems were used in a non-flight capacity for 5 of these incidents, and the remaining 4 incidents the UAS technology was deployed to an incident but not utilized in any capacity.

Of the 102 incidents, 13 of them were requests to support outside law enforcement agencies or city departments other than the San Diego Police Department. Of the 102 incidents, 10 of them were conducted in locations outside of the city of San Diego.

In 2024, the Dejero DTS was utilized at 63 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 (See below table for details).

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

CATEGORY (continued)	**DEJERO DTS**	**DIVISION**
Other (i.e. Inspections, Disaster Response, etc)	NO	Out of City
Special Events (Enhanced Security)	YES	NORTHERN
Special Events (Enhanced Security)	YES	NORTHERN
Special Events (Enhanced Security)	YES	NORTHERN
Special Events (Enhanced Security)	YES	CENTRAL
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	SOUTHERN
SAR - Search and Rescue for Missing Persons	NO	NORTHWESTERN
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	MIDCITY
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	MIDCITY
Crime Scene Evidence Collection	NO	EASTERN
SAR - Search and Rescue for Missing Persons	NO	NORTHEASTERN
Special Events (Enhanced Security)	YES	NORTHERN
Special Events (Enhanced Security)	YES	NORTHERN
Special Events (Enhanced Security)	YES	NORTHERN
Special Events (Enhanced Security)	YES	NORTHERN
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	SOUTHEASTERN
Crime Scene Evidence Collection	NO	EASTERN
Special Events (Enhanced Security)	YES	WESTERN
Special Events (Enhanced Security)	YES	CENTRAL
Special Events (Enhanced Security)	YES	CENTRAL
Special Events (Enhanced Security)	YES	CENTRAL
SWAT Support , High Risk Tactical Operation, or Suspect Search	NO	OUT OF CITY
Special Events (Enhanced Security)	YES	CENTRAL
Crime Scene Evidence Collection	NO	CENTRAL
Special Events (Enhanced Security)	YES	CENTRAL
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	SOUTHERN
Special Events (Enhanced Security)	NO	CENTRAL
Special Events (Enhanced Security)	NO	CENTRAL
Crime Scene Evidence Collection	NO	WESTERN
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	SOUTHERN
Special Events (Enhanced Security)	YES	NORTHERN
Special Events (Enhanced Security)	YES	NORTHERN
Special Events (Enhanced Security)	YES	NORTHERN
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	OUT OF CITY
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	OUT OF CITY
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	OUT OF CITY
Special Events (Enhanced Security)	YES	NORTHERN
SWAT Support , High Risk Tactical Operation, or Suspect Search	NO	SOUTHERN
Special Events (Enhanced Security)	YES	NORTHERN

CATEGORY (continued)	DEJERO DTS	DIVISION
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	SOUTHEASTERN
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	SOUTHEASTERN
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	CENTRAL
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	SOUTHEASTERN
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	NORTHERN
Special Events (Enhanced Security)	YES	NORTHERN
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	EASTERN
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	EASTERN
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	NORTHWESTERN
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	WESTERN
Special Events (Enhanced Security)	YES	CENTRAL
Special Events (Enhanced Security)	YES	CENTRAL
Special Events (Enhanced Security)	YES	CENTRAL
Special Events (Enhanced Security)	YES	CENTRAL
Crime Scene Evidence Collection	NO	SOUTHEASTERN
SAR - Search and Rescue for Missing Persons	NO	NORTHERN
Special Events (Enhanced Security)	YES	CENTRAL
Special Events (Enhanced Security)	YES	CENTRAL
SWAT Support , High Risk Tactical Operation, or Suspect Search	YES	SOUTHEASTERN
SWAT Support , High Risk Tactical Operation, or Suspect Search	NO	NORTHERN
Crime Scene Evidence Collection	NO	CENTRAL
Special Events (Enhanced Security)	NO	NORTHERN
Special Events (Enhanced Security)	NO	NORTHERN
SWAT Support , High Risk Tactical Operation, or Suspect Search	NO	NORTHERN

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

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

DATA BREACH OR UNAUTHORIZED ACCESS

SDPD is not aware of data breaches or unauthorized access to the data collected by these surveillance technologies.

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, selecting, and approving technology solutions. Cyber security and technology risks are also assessed by SDPD's 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 UAS Unit does not produce, collect or share crime statistics.

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.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

There was one Public Records Act requests regarding these surveillance technologies.

Request Number	Request Date	Closed Date
24-7535	10/28/2024	11/5/2024

ANNUAL COST

During the 2024 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 $63,091.06.
- California Seized Assets special funding source supported $9,042.39.
- State COPS special funding source supported $20,001.63.
- UASI Grant funding supported $453,155.42.

No new Dejero DTS hardware technology was procured this Calendar year. The current annual costs to support sim card data plans for these devices to operate is approximately $7,200.00.

REQUESTED MODIFICATIONS TO THE USE POLICY

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

San Diego Police Department Covert Technologies

SDPD

ONE TEAM. ONE MISSION.

San Diego Police Department

Covert Audio and Video Technology

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 was 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 are generally utilized through a phone line. The devices were used 128,814 times during the 2024 calendar year. The usage of the devices is tracked by each individual call or text. That number includes all the calls and texts recorded during each operation. Each operation can have numerous investigators utilizing the system at once.

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. The Department utilized 107 lines in the 2024 calendar year.

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 2024 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 not utilized during the 2024 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 five times during the calendar year 2024.

Power Over Ethernet 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 only utilized once during the calendar year 2024.

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 devises 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 2024 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 2024 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 use in their investigation(s).

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.

LOCATION

Most of the use for these devices are 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

There have been no updates, upgrades, or configuration changes that expanded or reduced the surveillance technology capabilities. Modems were exchanged, but there was no functionality or features added.

DEPLOYMENT LOCATION

This technology was utilized in all of the San Diego Police Department service areas. Most locations are confidential and are being withheld in compliance with the ordinance safeguards against releasing confidential or sensitive information.

The only use during the 2024 calendar year of the Power Over Ethernet Digital Video Recorder and Camera technology was of a subject leaving suspicious devices at a City of San Diego Fire Station in Golden Hill (Central Division). Cameras were set up to monitor the entrance of the fire station where the subject had been leaving the items. The subject could be seen dropping the items and then leaving westbound. The subject was identified with the assistance of the video.

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

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

DATA BREACH OR UNAUTHORIZED ACCESS

There were not any 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, 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 these technologies.

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.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

There were no Public Records Act requests regarding these technologies.

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 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.

Covert Cloud Based Mobile Application: The cost for this service is $23,984.76 a year.

Power Over Ethernet 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.

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

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

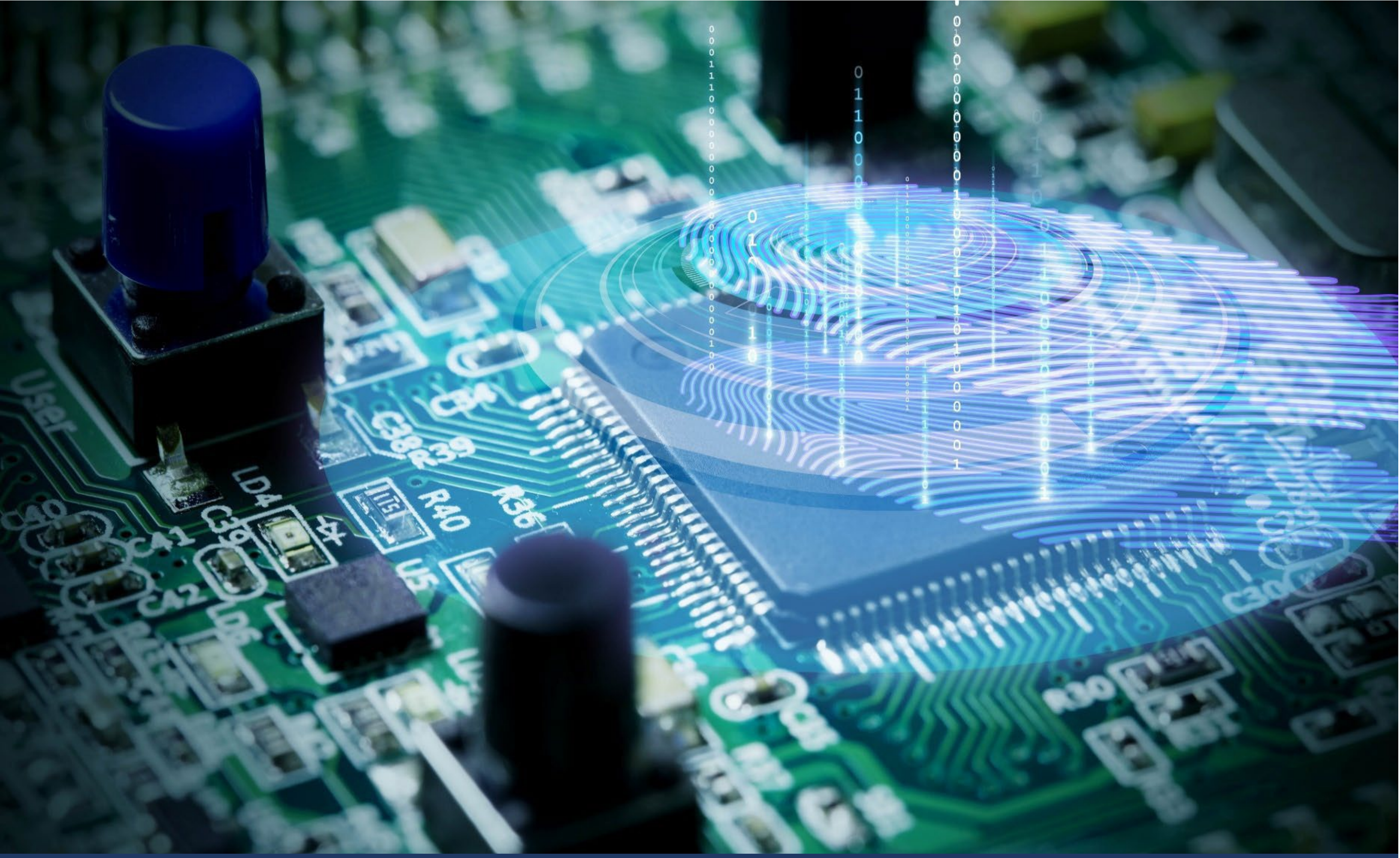
Trail Cameras: The units were a one-time fee to purchase. There are no annual costs for this technology.

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

The funding for these technologies was provided by a Justice Assistance Grant (JAG).

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 Cellebrite Premium/UFED and Physical Analyzer (now called Cellebrite Inseyets), 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 Premium/UFED (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 Physical Analyzer 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 140 terabytes (TB) of data were generated via MDFT in 2024, impacting over 350 investigations through the forensic extraction of approximately 576 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 Penal Code 1546.1].

Data that has been extracted using MDFT is not shared with external sources without a court order or other legal proceedings such as 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 Premium	Cellebrite Physical Analyzer	Magnet Axiom	Magnet Graykey
7.64.0.271	7.66.0.9	7.10.1.39284	1.17.7.26651541 / 3.30.0b2.26811624
7.65.404	7.67.0.15	8.0.0.39753	1.17.7.26651541 / 3.30.0.26870903
7.66.0.138	7.68.0.25	8.1.0.40287	1.17.7.26651541 / 3.30.0.26881838
7.68.0.809	7.69.0.10	8.2.0.40565	1.17.7.26651541 / 3.31.0b0.26941704
7.69.0.1397		8.3.0.41805	1.17.7.26651541 / 3.31.0.27012057
7.70.0.180		8.3.1.41227	1.17.7.26651541 / 3.32.0b0.27131744
		8.4.0.41469	1.17.7.26651541 / 3.32.0b4.27210103
		8.5.1.41927	1.17.7.26651541 / 3.32.1.27291815
		8.7.1.42615	1.20.0.27301552 / 3.33.0b5.27380103
			1.20.1.27412205 / 4.0.0b7.27551831
			1.20.1.27412205 / 4.0.0.27561855
			1.21.0.27571328 / 4.1.0b3.27691603
			1.21.0.27571328 / 4.1.0.27711255
			1.22.0.27801658 / 4.3.0.28061600
			1.22.0.27801658 / 4.4.0b3.28131828

Cellebrite Premium	Cellebrite Physical Analyzer	Magnet Axiom	Magnet Graykey
			1.22.0.27801658 / 4.4.0b4.28141809
			1.22.0.27801658 / 4.4.0b5.28190003
			1.22.0.27801658 / 4.4.0.28191612
			1.22.0.27801658 / 4.5.0b4.28392127
			1.22.0.27801658 / 4.5.0b5.28411541
			1.22.0.27801658 / 4.6.0b0.28431821
			1.22.0.27801658 / 4.6.0b3.28520142
			1.22.0.27801658 / 4.6.0.28551833
			1.23.0.28551906 / 4.7.0b2.28700003
			1.23.0.28551906 / 4.7.0.28811810
			1.23.0.28551906 / 4.8.0b1.28881331
			1.23.0.28551906 / 4.8.0b3.28902019
			1.24.0.28720042 / 4.9.0b1.29021511
			1.24.1.29051749 / 4.9.0.29131810
			1.24.1.29051749 / 5.0.0b0.29191357
			1.24.2.29241656 / 5.1.0.29371940
			1.24.2.29241656 / 5.2.0b2.29401809
			1.24.2.29241656 / 5.2.0b4.29461826
			1.24.2.29241656 / 5.2.0b10.295300002
			1.24.2.29241656 / 5.3.0b6.29672002
			1.24.2.29241656 / 5.3.0.29721313
			1.24.2.29241656 / 5.4.0b3.29821222
			1.24.2.29241656 / 5.5.0.29941342
			1.24.2.29241656 / 5.5.1.30021836
			1.24.2.29241656 / 5.6.0b2.30181931
			1.25.0.30192015 / 5.6.0.30251529

DEPLOYMENT LOCATION

The MDFT are only deployed in secured rooms at SDPD headquarters.

COMMUNITY COMPLAINTS OR CONCERNS

SDPD is committed to protecting the civil rights and liberties of our citizens as presented to the City Council for approval of this technology. SDPD 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

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

DATA BREACH OR UNAUTHORIZED ACCESS

There were 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, selecting, and approving technology solutions. Cyber security and technology risks are also assessed by SDPD's 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 these technologies.

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.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

There was one Public Records Act request. The open and close dates are as follows:

CPRA #	Open Date	Close Date
24-5098	7/26/24	8/5/24

ANNUAL COST

The approximate costs of the MDFT for 2024 total $177,126.81 and were paid via the general fund. The cost per technology is listed below:

- Cellebrite UFED/Premium: $133,369.38

Magnet Graykey:	$30,717.43
Magnet Axiom:	$13,040

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

REQUESTED MODIFICATIONS TO THE USE POLICY

Cellebrite renamed their UFED suite of tools to Inseyets. Staffing in the FTU also expanded in 2024. FTU staff who are not criminalists may be trained to utilize the technologies to support the work of the unit. Therefore, the draft modified Use Policy has been amended to reflect the product name and personnel description change.

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 San Diego Police Department Emergency Negotiations Team utilizes the 836 Technologies Tactical Throw Phone and the 836 Technologies CINT Commander II 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 potentially life-threatening incidents to a peaceful resolution.

Neither the 836 Technologies Tactical Throw Phone nor the 836 Technologies CINT Commander II was utilized during the 2024 calendar year.

SHARING OF DATA

No data was acquired by the 836 Technologies Tactical Throw Phone or the 836 Technologies CINT Commander II during the 2024 calendar year.

LOCATION

Neither the 836 Technologies Tactical Throw Phone nor the 836 Technologies CINT Commander II was utilized during the 2024 calendar year.

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

Neither the 836 Technologies Tactical Throw Phone nor the 836 Technologies CINT Commander II was utilized during the 2024 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.

AUDITS OR INVESTIGATIONS

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

DATA BREACH OR UNAUTHORIZED ACCESS

The Department is not aware of data breaches or unauthorized access to the data collected by these surveillance technologies.

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, 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 these technologies.

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.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

There were no Public Records Act requests regarding these technologies in 2024.

ANNUAL COST

There were no associated costs for the use of the 836 Technologies Tactical Throw Phone or the 836 Technologies CINT Commander II during the 2024 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.

San Diego Police Department

Berla iVe Toolkit

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

The Berla equipment was used 10 times in 2024.

SHARING OF DATA

Each of the ten uses of the Berla equipment in 2024 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 the SDPD. No uses were for agencies outside the Department. Of the ten BERLA downloads from 2024, three belonged to Traffic Investigations. Of the three, one is still under investigation and will be sent forward to the District Attorney's (DA) Office at a later date. Another had incomplete information and could not be sent forward to the DA's Office, and the third case was submitted to the DA's Office with BERLA disclosure in the investigator follow-up.

The seven other BERLA downloads were done for other SDPD units and provided to the assigned investigator. Of those cases, all but one were sent forward to the DA's Office. One was unable to be completed due to the responding unit being disabled on the subject vehicle.

LOCATION

The Berla equipment is kept in a locked cabinet in a Department facility 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 2024, Berla issued five software updates:

- 4.6 – Additional support for Toyota vehicles
- 4.7 – Additional supported for Volkswagen and Toyota vehicles
- 4.8 – Enhanced acquisitions for Stellantis vehicles

- 4.9 – Expanded support for Honda vehicles
- 4.10 – Added support for Hyundai vehicles

DEPLOYMENT LOCATION

Use of the Berla equipment is done on vehicles that were impounded as evidence and stored at SDPD Traffic Division; therefore, the equipment does not need to be deployed to outside locations. Traffic Division is located in the Eastern Division police service area.

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 and has not received any reports of disproportionate impacts. The Use Policy continues to protect civil rights and civil liberties.

AUDITS OR INVESTIGATIONS

A log is kept of those investigators that 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. There were no reported violations of the Surveillance Use Policy or SDPD Policy or Procedure regarding this technology.

DATA BREACH OR UNAUTHORIZED ACCESS

There have been no known data breaches or unauthorized access to the data collected by the surveillance technology.

DATA BREACH DETECTION

The Berla equipment is not connected to a network.

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

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

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.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

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

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.

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 a 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 subject's cell phone in relation to a criminal investigation.

238 cases with 4,131 location-based files were successfully uploaded into the system in 2024.

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.

Files can be viewed by either Detectives or Crime Analysts that upload records into the system, sometimes working in conjunction with one another on an investigation. Analytical byproducts produced from the use of the technology may be included in investigative submission packets shared with the District Attorney's office for criminal proceedings.

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 would only be granted on a specific basis for work on a specific case and not be granted for the entire agency's available data.

LOCATION

CellHawk is a web-based application. There are no local programs or hardware installed for this technology on any Department computers.

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 surveillance technology is accessed by centralized investigative units and Crime Analysis, primarily based at the SDPD's headquarters (Central Division service area), and Traffic (Eastern Division service area). However, as a web-based application, it can be accessed from other department locations citywide.

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 and has not received any reports of disproportionate impacts. The Use Policy continues to protect civil rights and civil liberties.

AUDITS OR INVESTIGATIONS

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

DATA BREACH OR UNAUTHORIZED ACCESS

The Department is not aware of data breaches or unauthorized access to the data collected by this 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, 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

While this technology is used in support of active criminal investigations, there is no direct correlation between the use of CellHawk and overall Citywide crime statistics.

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.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

There were no Public Records Act requests regarding this technology.

ANNUAL COST

CellHawk's cost to the SDPD is approximately $19,800 per fiscal year, and is a recurring cost factored into the SDPD's 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.

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.

16,307 searches were conducted within the tool by Department personnel in 2024.

TLOxp is an internet-based, online service provided by TransUnion. As defined on TLO.com, "TLOxp® is the latest generation of the technology that originated the science of data fusion. Built on an architecture of supercomputers running proprietary linking and assessment algorithms, TLOxp filters through a massive repository of public and proprietary data almost instantly." It offers real-time resources to locate information about individuals, utilities, and assets. It is used to support San Diego Police Department criminal investigations.

61,363 searches were conducted within the tool by Department personnel in 2024.

SHARING OF DATA

Reports provided by the CP Clear and TLOxp systems are compiled using already existing publicly available 3rd party datasets acquired by both vendors. Records can be viewed by either Detectives or Crime Analysts that generate reports from the system, sometimes working in conjunction with one another on an investigation. Analytical byproducts produced from the use of the technology may be included in investigative submission packets shared with the District Attorney's office for criminal proceedings.

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

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

DEPLOYMENT LOCATION

These surveillance technologies are accessed by centralized investigative units and Crime Analysis, based at the SDPD's headquarters (Central Division service area), and by area station investigators from their respective commands located within the City.

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

There were no reported violations of the Surveillance Use Policy or SDPD Policy or Procedure regarding these technologies.

DATA BREACH OR UNAUTHORIZED ACCESS

The Department is not aware of data breaches or unauthorized access to the data collected by these surveillance technologies.

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, 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

While these technologies are used in support of active criminal investigations, there is no direct correlation between the use of CP Clear/TLOxp and overall Citywide crime statistics.

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.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

There were no Public Records Act requests regarding these technologies.

ANNUAL COST

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

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

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. The Nighthawk system was accessed 2,214 times by its registered users in the 2024 calendar year.

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.

If the user, a detective or crime analyst, requests assistance from a Nighthawk analyst for assistance on either uploading a file into the system or interpreting the results once an upload is complete, the files retained in the system can be accessed by Nighthawk analysts.

Every investigator or analyst assigned a Nighthawk license are 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 2024.

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 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 and has not received any reports of disproportionate impacts. The Use Policy continues to protect civil rights and civil liberties.

AUDITS OR INVESTIGATIONS

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

DATA BREACH OR UNAUTHORIZED ACCESS

The Department is not aware of data breaches or unauthorized access to the data collected by this 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, 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 these technologies.

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.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

There were no Public Records Act requests regarding this technology.

ANNUAL COST

The cost for the service is $87,960 a year. This amount is the cost of the service for FY2025 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 are no requested modifications to this technology's 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.

During the year 2024, Realquest Online Services were utilized approximately five 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 changes that expanded or reduced the surveillance technology capabilities.

DEPLOYMENT LOCATION

This surveillance technology was deployed by the Abandoned Vehicle Abatement Unit for all police service areas. The surveillance technology, Realquest Online Services, was only accessed from secure department computers via user login authentication.

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 and has not received any reports of disproportionate impacts. The Use Policy continues to protect civil rights and civil liberties.

AUDITS OR INVESTIGATIONS

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

DATA BREACH OR UNAUTHORIZED ACCESS

The Department is not aware of data breaches or unauthorized access to the data collected by this 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, 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. 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.

Realquest Online Services was utilized five times for the purpose of obtaining contact information of a property owner and was successful in gaining compliance by all five owners to move the vehicle and avoid further proceedings.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

There were no Public Records Act requests regarding this technology.

ANNUAL COST

The Realquest Online Services annual subscription costs approximately $2,397, 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 to this technology’s Use Policy.

San Diego Police Department

Vigilant: Automated License Plate Recognition (ALPR)

Department/Division: Police - Watch Commander

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 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 and has not received any reports of disproportionate impacts. The Use Policy continues to protect civil rights and civil liberties.

AUDITS OR INVESTIGATIONS

A supervisor of the Special Projects and Legislative Unit conducted weekly audits of the system. Any identified discrepancies with metadata entries were immediately addressed with the user.

- All documentation provided to officers regarding improper use of the system is considered a personnel record and not subject to disclosure per California Penal Code section 832.7 and California Evidence Code section 1043 (peace officer personnel records).

DATA BREACH OR UNAUTHORIZED ACCESS

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

DATA BREACH DETECTION

The City's Department of Information Technology (IT) 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

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

INFORMATION AND STATISTICS

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.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

There were no Public Records Act requests regarding this technology.

ANNUAL COST

For CY 2024 a payment of $2,600 was made on 08-01-2024 for the non-commercial version.

For CY 2025 the cost of access to the commercial version of Vigilant will be $54,750.

All funding sources are from the City General Fund.

REQUESTED MODIFICATIONS TO THE USE POLICY

There are no requested modifications to this technology’s 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 Observation Tower provides a raised platform for viewing by up to two personnel. This unit is equipped with one pan tilt zoom (PTZ) camera and can provide real-time video to the person occupying Skywatch during an incident. The SKYWATCH Tower is used for live situational awareness, enhanced security overwatch during large events and gatherings and as a visual deterrent. In 2024, this technology was used during seven 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, and 7). The surveillance technology was used for live situational awareness, enhanced security overwatch during large events and gatherings and as a visual deterrent. In 2024, this technology was used during 19 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 2024, this technology was used during 13 events.

SHARING OF DATA

The Logistical Support Unit received no data-sharing requests from these surveillance technologies during the 2024 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.

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)	Western 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)	Western Division	Special Event Operations
Command Vehicle (ARTECO)	Northern Division	Special Event Operations
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)	Northeastern Division	Special Event Operations
Command Vehicle (ARTECO)	Western Division	Special Event Operations
Command Vehicle (ARTECO)	Central Division	Special Event Operations
Command Vehicle (ARTECO)	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	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
Camera Trailers	Central Division	Special Event Operations
Camera Trailers	Harbor Police Department	Special Event Operations

Equipment Type	Deployment Area	Reason for Deployment
SKYWATCH Observation Tower	Western Division	Special Event Operations
SKYWATCH Observation Tower	Central Division	Special Event Operations
SKYWATCH Observation Tower	Western Division	Special Event Operations
SKYWATCH Observation Tower	Central Division	Special Event Operations
SKYWATCH Observation Tower	Western Division	Special Event Operations
SKYWATCH Observation Tower	Northeastern Division	Special Event Operations
SKYWATCH Observation Tower	Central Division	Special Event Operations

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

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

DATA BREACH OR UNAUTHORIZED ACCESS

The Department is not aware of data breaches or unauthorized access to the data collected by these surveillance technologies.

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, 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 these technologies.

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.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

There were no Public Records Act requests regarding these technologies in 2024.

ANNUAL COST

$25,000.00 Annual software & up-date through Aggerate Way.

$25,000.00 Annual maintenance through DVR Simple Solutions.

$25,000.00 Annual parts through Willy's Electronic Supply. This technology is paid for

through the City's General Fund.

REQUESTED MODIFICATIONS TO THE USE POLICY

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

San Diego Police Department

Automated License Plate Recognition (ALPR)

Department/Division: Police - Special Project and Legislative Affairs

Related Policy/Procedure:

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

Revised October 23, 2025

DESCRIPTION

This revised Annual Report provides an overview of how Automated License Plate Recognition (ALPR) technology enhances public safety in the City of San Diego (City). It explains how the system works, how the San Diego Police Department (SDPD) uses it responsibly, and how it supports investigations while protecting privacy and civil liberties. The report also highlights improvements developed in collaboration with the Privacy Advisory Board (PAB).

Automated License Plate Recognition (ALPR) technology uses cameras and software provided by the vendor, Flock, to automatically identify and record rear-mounted license plates. Cameras mounted on streetlights at 500 locations across the City capture images of passing or parked vehicles in public places.

The system reads each plate number, notes the time, date, and location, and may record general vehicle characteristics such as make, model, and color. This information is encrypted and transmitted to a secure database that only authorized SDPD personnel can access. The technology operates continuously, not to monitor individuals, but to help locate vehicles linked to crimes, missing persons, or public safety alerts quickly and accurately. A plate that seems ordinary today may become crucial evidence tomorrow when a crime is reported.

Although the system collects a large amount of data, the vast majority is never viewed by approved SDPD personnel and is automatically deleted within 30 days unless it becomes evidence in an active case.

In 2024:

- Officers conducted more than 140,000 investigative searches of ALPR data, which played a key role in 294 cases.
- The technology supported the arrest of 208 suspects and the recovery of 10 firearms and approximately $3 million in stolen property, including 223 stolen vehicles.
- Of the 35 homicides San Diego experienced in 2024, ALPR technology aided in a third of them and helped lead to six apprehensions. Four of those cases would not have been solved without the technology’s assistance.
- ALPR also helped locate a missing man with dementia, apprehend a suspect wanted for the attempted kidnapping of two children, and identify suspects in a series of hate crimes in Hillcrest.
- Beyond arrests, ALPR improves precision policing – helping officers rely on verified

information rather than broad patrols, which reduces unnecessary community contacts, conserves resources, and increases safety for both officers and residents.

SDPD's use of ALPR technology is guided by clear policy standards that were developed in partnership with the PAB and strictly define when and how the system may be used. These safeguards are codified in the ALPR Use Policy, ensuring that the technology serves legitimate public safety purposes while protecting privacy and civil rights.

The Automated License Plate Recognition (ALPR) system may only be used for official law enforcement purposes such as locating vehicles connected to investigations, supporting responses to critical incidents, and assisting in efforts to find at-risk missing persons. These uses ensure that ALPR technology remains a focused investigative and public safety tool rather than a system for general surveillance. A complete description of authorized uses is provided in the ALPR Use Policy.

The Use Policy also establishes clear prohibitions to prevent misuse and protect individual rights. ALPR data and cameras may not be used to invade personal privacy, discriminate or target individuals or groups, violate constitutional or statutory protections, or serve any personal or non-law enforcement purpose.

These restrictions are reinforced through SDPD training, audits, and system access controls. Each authorized user must complete ALPR-specific training on lawful use, privacy, and data handling before being granted system access. Violations of these provisions are subject to disciplinary action and review.

By codifying these standards, SDPD ensures ALPR use remains narrowly focused on legitimate law enforcement needs. The Use Policy's structure, clearly distinguishing authorized and prohibited uses, creates transparency, consistency, and accountability. Together with California Senate Bill 34, California Senate Bill 54 and the City's Transparent and Responsible Use of Surveillance Technology (TRUST) Ordinance, these internal protections demonstrate SDPD's commitment to balancing public safety with the privacy and civil rights of all San Diegans.

ALPR has proven to be a force multiplier for SDPD. Although it is difficult to measure precisely how much time or labor the system saves because no standardized baseline existed before its implementation, case examples and investigator feedback consistently show that ALPR improves efficiency and investigative success. Please see Addendum B, which provides a monthly breakdown of system use and specific case examples where ALPR technology assisted investigations.

Through continued collaboration with the PAB and strict adherence to City and State privacy laws, San Diego remains a national leader in the transparent, accountable, and effective use of ALPR technology.

SHARING OF DATA

In addition to providing ALPR data to the District Attorney's Office for criminal prosecution, SDPD accessed or shared ALPR images or data with other law enforcement agencies after a qualifying crime had occurred, such as a homicide or shooting, and when there was a legitimate investigative need.

In a few serious cases in 2024, involving crimes such as human trafficking, an assault against an officer and crimes against children, SDPD shared ALPR data with out-of-state and federal law enforcement agencies. None of the qualifying crime cases were related to immigration enforcement. (See Addendum A for a comprehensive list of outside agency data sharing.)

After receiving guidance from the California Department of Justice, SDPD immediately ended all such sharing with federal and out-of-state departments. This decision was formalized in a Department-wide order in May 2025.

Additionally, SDPD identified a brief period after system launch during which other California law enforcement agencies could temporarily access SDPD's ALPR data. As SDPD discussed in a memo issued to the PAB and each member of City Council on June 13, 2025, this period was mistakenly left out of the original Annual Surveillance Report and has been added to the Unauthorized Access section below.

These changes reflect SDPD's commitment to responsible technology use and public trust.

UPDATES, UPGRADES, AND CONFIGURATION CHANGES

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

ANNUAL COST

**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 Automated License Plate Recognition (ALPR) cameras.

In 2024, the City of San Diego paid a one-time installation and activation fee of $1,500,000. This fee covered:

1. Installation of 500 Smart Streetlight units, along with any future units approved by City Council, at designated locations.
2. Removal of existing CityIQ units from locations where the new system was deployed, and the safe transfer of those units to City storage.
3. Installation of the new units and initiation of service in accordance with the project milestone schedule.

No additional activation fees will be required for any future units authorized by City Council.

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

On December 26, 2023, the City issued an initial payment of $3,512,500, which included the $1.5 million installation fee and the first year of service for all 500 Smart Streetlights and ALPR cameras.

Due to City infrastructure needs, a $6,800 payment was made on June 24, 2024, to relocate several Smart Streetlight units. The relocation cost was $450 per camera, as specified in the contract.

Between installation, activation, and relocation costs, the total amount paid for the 2024 Smart Streetlight Program was $3,519,300.

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.

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

A copy of the full contract, COSD Public Safety Agreement – Ubicquia, is available at cosd-public-safety-agreement-ubicquia.pdf.

LOCATION

The Smart Streetlights System, which includes the situational cameras and the ALPR cameras, were attached to City of San Diego streetlight poles.

DEPLOYMENT LOCATION

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

Since SDPD's ALPR program launched, some community members have raised concerns over how the technology protects people's privacy, if it could be used in immigration or reproductive rights investigations, and whether the data collected would be vulnerable to outside access.

SDPD has taken these concerns seriously. SDPD has worked to educate the public, strengthen policies, and partner closely with the PAB to ensure the community can feel confident this technology is being used responsibly to keep our neighborhoods safe.

Additionally, SDPD received a letter dated July 31, 2024, from the Community Advocates for Just and Moral Governance titled "Notice of Violations of the TRUST Ordinance – Smart Streetlights and Automated License Plate Readers." No other written complaints or concerns have been filed with SDPD.

SDPD remains committed to working with community groups, the Privacy Advisory Board, and elected officials to ensure continued public education and transparency around this technology. The Use Policy continues to outline clear safeguards to protect civil rights and civil liberties.

AUDITS OR INVESTIGATIONS

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 the San Diego Police Department. 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.

To maintain certification, all authorized users must complete annual ALPR training through the City's training portal. If training is not completed on time, system access is automatically suspended until the user submits a valid certificate of completion to the program administrator.

These regular audits and training requirements ensure that SDPD maintains full accountability and compliance in its use of ALPR technology.

SDPD's audit work drove key improvements to Flock's software, including one piloted in San Diego that has since evolved into a network-wide standard.

In the Flock Safety interface, users conducting a search of ALPR data were required to enter a "Reason" for the search, but it did not prompt users to include a case or incident number. Because of this, users provided appropriate reasons for a search, which is in line with SDPD's Surveillance Use Policy, but because there was not a more detailed prompt, more specific information was omitted.

To address this, on January 26, 2024, the audit issued ORDER OR 24-04, which requires all ALPR users to:

- Include a specific case number or incident number in the "reason" field when conducting searches.
- Ensure the event is linked to a specific crime (broad entries like "11-86" are no longer acceptable).
- Add relevant details to assist with investigative documentation and future

court proceedings.

Because this update was implemented after the system launch, it took users time to adjust. However, any time a user conducted a search without the appropriate metadata, a supervisor immediately addressed the issue. Those searches were verified to be connected to an active case number or event number in compliance with the Use Policy.

After the Department Order was issued, fewer than one percent of searches were missing the required metadata.

SDPD worked with Flock Safety to create a new, dedicated "Case/Incident Number" field in addition to the "reason" field. This section was added to the Flock Safety interface nationwide, resulting in more thorough entries and audits.

The Department Order is part of this year's Annual Training related to the ALPR system and will be rolled into annual training moving forward.

As previously discussed, another type of internal audit identified the period at our system's launch when an improper setting mistakenly allowed California law enforcement agencies to access SDPD's ALPR data in late December 2023 to early January 2024. That setting was immediately corrected and hasn't occurred since.

This incident motivated SDPD to build on its audit process by including SDPD's Research, Analysis and Planning Unit (RAP) (SDPD's internal auditing and controls unit) earlier in the process and by mandating quarterly audits. On April 25, 2025, a Department Order was issued requiring surveillance technology Subject Matter Experts (SME) to conduct these enhanced audits.

As part of this process:

- All SMEs will conduct quarterly audits of the requirements in the Annual Report to enhance record keeping and ensure greater accuracy of the Annual Report.
- SDPD SMEs will conduct audits at random for uses of the technology.
- SDPD will create share logs to document what data is shared and why.
- RAP will conduct independent audits to confirm share logs are completed, ensure that use policies are current, and ensure that system user access is up to date. Any violation will be immediately reported to RAP for documentation and corrections.

DATA BREACH DETECTION

SDPD works closely with the City's Department of Information Technology (IT) to assess cybersecurity risks, approve technology, and ensure proper governance. Additional details about the City's IT governance processes can be found in the FY23–FY27 IT Strategic Plan.

Key safeguards include:

Secure Cloud Storage: All ALPR data is stored on the Amazon Government Cloud, which includes multiple layers of digital protection.

Encryption and Firewalls: Data is safeguarded with encryption, firewalls, and multi-factor authentication protocols to protect digital evidence.

Controlled Access: Access is limited to SDPD personnel assigned to investigative or enforcement roles. Only individuals authorized by the Chief of Police are permitted to access ALPR data.

Secure Access Management

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 user name, 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.

Vendor Security Standards

Flock Safety, the City's ALPR technology provider, follows strict cybersecurity protocols and undergoes regular third-party audits. Flock's system operates on Amazon Web Services (AWS), a cloud platform designed for government-level security. The company employs 256-bit encryption, role-based access, and full Criminal Justice Information Services (CJIS) compliance.

Flock Safety maintains multiple third-party cybersecurity certifications, including:

- SOC 2 Type II – Systems and Organization Controls (AICPA)
- SOC 3 – Public report of internal controls for security and availability
- ISO 27001:2022 – Information security management systems (International Standards Organization)
- NIST 800-53 / Rev. 5 – Security and privacy controls for information systems (National Institute of Standards and Technology)
- HIPAA – Health Insurance Portability and Accountability Act compliance
- VPAT – Voluntary Product Accessibility Template (Information Technology Industry Council)
- CISA Secure by Design Pledge – Cybersecurity & Infrastructure Security Agency initiative

IT Governance and Certification

In 2023 prior to installation, the Flock ALPR solution underwent review through the Department of Information Technology's Governance Process, in accordance with Administrative Regulation (AR) 90.68 – Procurement of Technology Solutions. Flock's system demonstrated alignment with the City's technical and security standards and received full approval.

In addition to meeting City IT governance requirements, Flock Safety adheres to all applicable cybersecurity industry standards, attestations, and frameworks listed above.

DATA BREACH OR UNAUTHORIZED ACCESS

Although California law permits ALPR database access between California agencies, the City's Contract and Use Policy for ALPR bars outside agencies from accessing SDPD's ALPR Flock database. While there was no data breach, there was a brief period of unauthorized access by other California law enforcement agencies due to a system configuration error at the system's launch.

As a result of the system misconfiguration, from December 29, 2023, to January 17, 2024, SDPD's ALPR camera system was inadvertently included in 12,914 searches conducted by other state agencies. No out-of-state or federal law enforcement agencies had access to data during this period. While an additional 795 searches were conducted on December 28, 2023, none of SDPD's cameras had been turned on, so there was no data available to search.

Of the 12,914 searches conducted by other state agencies, 12,202 were for a specific license plate or partial license plate, and around 50 percent were repeated inquiries for the same license plate wanted in connection with a criminal investigation.

Below is a table showing the number of cameras active on each day and the number of searches conducted by other state agencies:

Date	Active Cameras	Searches
28-Dec	0	795
29-Dec	7	1099
30-Dec	7	462
31-Dec	7	717
1-Jan	7	231
2-Jan	7	592
3-Jan	9	1060
4-Jan	10	1040

5-Jan	13	655
6-Jan	13	554
7-Jan	13	343
8-Jan	21	571
9-Jan	26	922
10-Jan	32	981
11-Jan	35	898
12-Jan	35	514
13-Jan	35	458
14-Jan	35	200
15-Jan	35	379
16-Jan	39	635
17-Jan	41	503

Search Timeframe	Number of Searches
2023 Searches	3,073
2024 Searches	10,536
Total	**13,609**
December 28, 2023, Searches	-795
Actual Searches	**12,914**

The initial unauthorized access was discovered through an internal audit on or around January 17, 2024. SDPD immediately notified Flock, which corrected the data-sharing settings the same day. This issue has not occurred since. (Please see Addendum A for a more detailed breakdown.)

INFORMATION AND STATISTICS

Quantitatively measuring the full impact of Automated License Plate Reader (ALPR) technology 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, while investigators consistently report that ALPR dramatically reduces time spent identifying suspect vehicles and coordinating responses, there is no pre-existing benchmark for how long these tasks took before the system was deployed.

Despite the absence of historical baselines, qualitative and case-based evidence strongly demonstrate the system’s effectiveness. ALPR has repeatedly enabled detectives to connect multi-jurisdictional crimes, locate violent offenders, and recover stolen property with greater speed and accuracy. In one case, investigators used ALPR data to identify a burglary suspect whose vehicle was tied to multiple crimes across several communities, an arrest that likely would have required weeks of manual follow-up without the technology. In another, a kidnapping victim was found safe within minutes of an ALPR alert pinpointing the suspect vehicle’s location. In addition, homicide, robbery, and child exploitation cases were solved through coordinated ALPR hits and Smart Streetlight camera footage that provided investigators with critical, time-sensitive leads. (Please see additional case information in Addendum B.)

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 20 percent in the year the technology was installed and continues to decline. This trend suggests that ALPR not only helps solve crimes after they occur but also acts as a deterrent by increasing the likelihood of recovery and arrest.

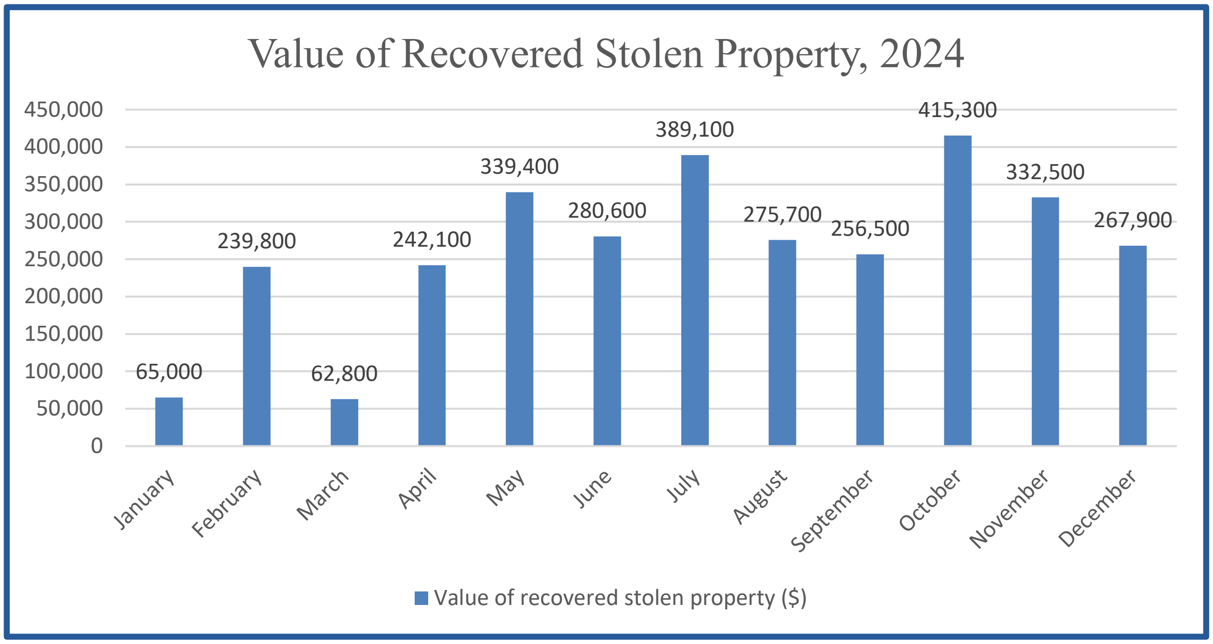
Taken together, these examples illustrate that ALPR functions as a powerful investigative multiplier, helping officers focus on credible leads, preventing further victimization, and enhancing community safety while reducing the need for broad or intrusive patrol activity.

While future reports may include new performance benchmarks, such as average time-to-identification or case clearance rates, the consistent outcomes across hundreds of investigations have demonstrated that ALPR technology is an indispensable, responsible, and effective tool in modern policing.

Investigation Assists	
187 PC – Homicide	11
211 PC – Robbery	6
207 PC – Kidnapping	3
245DV PC – Assault with a Deadly Weapon (Domestic Violence)	1
245 PC – Assault with a Deadly Weapon	5
261 PC – Rape	2
288 PC – Lewd or Lascivious Acts with a Child	3
459 – Burglary	10
Traffic (Serious Injury Crashes)	3
Other	10

ALPR Responses	
Stolen Vehicles Recovered	223
Stolen Vehicle Suspects In Custody	175
Missing Persons	1

Totals	
Total Events	294
Total Suspect In Custody	208
Estimated Value of Recovered Stolen Property	$3,055,400
Recovered Guns	10



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

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

There were five Public Records Act requests related to ALPR in calendar year 2024. 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
24-1400	2/23/2024	4/16/2024
24-6236	9/10/2024	9/14/2024
24-6912	10/6/2024	10/20/2024

24-7450	10/24/2024	10/24/2024
24-7913	11/12/2024	11/16/2024

REQUESTED MODIFICATIONS TO THE USE POLICY

The following modifications to the ALPR Use Policy are proposed.

- Add reference to California Senate Bill 34 under the subsection that defines prohibited ALPR uses including those that violate federal, state or local laws.
- Clarification 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.

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.

The only exception to this process occurred during the three-week period following system launch when a configuration error temporarily allowed other California law enforcement agencies to search SDPD's system directly. That issue was identified and fixed in January 2024.

SEARCHES CONDUCTED DURING THREE-WEEK LAUNCH PERIOD

California Agency	Times Shared
Alameda County Sheriff's Office	307
Alhambra Police Department	31
Anaheim Police Department	11
Anderson Police Department	4
Atherton Police Department	1
Auburn Police Department	4
Azuza Police Department	1
Bakersfield Police Department	5
Baldwin Park Police Department	33
Beaumont Police Department	71
Bell Gardens Police Department	1
Benicia Police Department	7
Beverly Hills Police Department	5
Brea Police Department	14
Brisbane Police Department	3
Buena Park Police Department	59
Burbank Airport Police Department	4
Burbank Police Department	21
Chino Police Department	56
Cal Fire	10
Cal State Fullerton	1
California Highway Patrol	91
Campbell Police Department	1
Capitola Police Department	33
Cathedral City Police Department	4
Citrus Heights Police Department	8
City of Riverside Police Department	11
Claremont Police Department	2
Colma City Police Department	6
Concord Police Department	2
Contra Costa County Sheriff's Office	168

Corona Police Department	102
Costa Mesa Police Department	10
Covina Police Department	65
Culver City Police Department	26
Cyprus Police Department	26
Danville Police Department	22
Delano Police Department	4
Dixon Police Department	12
East Bay Parks	12
El Cajon Police Department	2
El Centro Police Department	33
El Monte Police Department	220
Elk Grove Police Department	18
Escalon Police Department	8
Escondido Police Department	12
Fairfield Police Department	28
Farmersville Police Department	2
Folsom Police Department	10
Fontana Police Department	153
Fort Bragg Police Department	2
Freemont Police Department	24
Galt Police Department	5
Garden Grove Police Department	144
Gilroy Police Department	40
Glendale Police Department	8
Glendora Police Department	61
Grass Valley Police Department	11
Hanford Police Department	7
Hayward Police Department	60
Hemet Police Department	4
Hercules Police Department	69
Hillsborough Police Department	2
Hollister Police Department	1
Huntington Beach Police Department	25
Imperial City Police Department	1
Imperial County Sheriff’s Office	1
Indio Police Department	18
Irvine Police Department	104
Kern County Sheriff’s Office	257
Kings County Sheriff’s Office	17
La Habra Police Department	5
Laverne Police Department	5
Laguna Beach Police Department	36
Los Angeles County Sheriff’s Office	564
Lincoln Police Department	2
Lindsay Public Safety Department	5
Livermore Police Department	35
Lodi Police Department	14
Los Angeles Police Department	104

Madera County Sheriff’s Office	1
Marin County Sheriff’s Office	9
Mendocino County Sheriff’s Office	2
Menifee Police Department	1
Menlo Park Police Department	32
Merced County Sheriff’s Department	8
Monrovia Police Department	18
Montclair Police Department	36
Monterey County Sheriff’s Office	7
Monterey Park Police Department	1
Moraga Police Department	7
Morgan Hill Police Department	150
Mountain View Police Department	31
Murrieta Police Department	220
Napa County Sheriff’s Office	77
Northern California Regional Intelligence Center	53
Newark Police Department	21
Newport Beach Police Department	9
Novato Police Department	1
Oakley Police Department	16
Orange County Sheriff’s Office	1225
Oceanside Police Department	8
Ontario Police Department	69
Orange Police Department	37
Orange County District Attorney’s Office	8
Oxnard Police Department	21
Palm Springs Police Department	20
Palo Alto Police Department	23
Pasadena Police Department	1
Placentia Police Department	22
Placer County Sheriff’s Office	56
Pleasanton Police Department	1
Pomona Police Department	51
Porterville Police Department	11
Redlands Police Department	8
Redwood City Police Department	83
Rialto Police Department	15
Rio Vista Police Department	53
Riverside County District Attorney’s Office	19
Riverside County Sheriff’s Office	2037
Rocklin Police Department	12
Sacramento District Attorney’s Office	10
Sacramento Police Department	20
Salinas Police Department	3
San Bernadino County Sheriff’s Office	208
San Bruno Police Department	122
San Diego Sheriff’s Office	117
San Francisco Police Department	121
San Juaquin County Sheriff’s Office	145

San Leandro Police Department	3
San Louis Obispo Police Department	7
San Mateo Police Department	60
San Mateo County Sheriff’s Office	284
San Ramon Police Department	17
Santa Barbera County Sheriff’s Office	270
Santa Clara Police Department	202
Santa Cruz Police Department	2
Santa Maria Police Department	36
Santa Monica Police Department	1
Santa Rosa Police Department	60
Seal Beach Police Department	1
Simi Valley Police Department	10
Solano County Sheriff’s Office	255
Sonoma County Sheriff’s Office	91
Stockton Police Department	33
Suisun City Police Department	2
Torrance Police Department	1
Tracy Police Department	84
UC Riverside Police Department	1
Ukiah Police Department	15
Union City Police Department	4
Upland Police Department	80
Vacaville Police Department	31
Vallejo Police Department	21
Ventura Police Department	62
Ventura County Sheriff’s Office	41
Vernon Police Department	5
Visalia Police Department	57
Watsonville Police Department	25
West Covina Police Department	99
Wes Sacramento Police Department	3
Westminster Police Department	20
Whittier Police Department	6
Willits Police Department	2
Woodlake Police Department	26
Yreka Police Department	4

SEARCHES CONDUCTED BY SDPD FOR A CALIFORNIA AGENCY

California Agency	Times Shared
Alameda County Sheriff's Office	1
Anaheim Police	1
Belmont Police	1
Cal Automated Fingerprint Identification System	3
California Highway Patrol	19
Carlsbad Police	8
Chula Vista Police	51
Crime Stoppers	1
El Cajon Police	21
Escondido Police	6
Eureka Police	1
Huntington Beach Police	2
Imperial City Police	1
Indio Police	1
La Mesa Police	16
Long Beach Police	1
Los Angeles Airport Police	1
Los Angeles District Attorney's Office	1
Murietta Police	2
National City Police	61
Oceanside Police	7
Orange County Sheriff's Department	1
Redland Police	1
San Diego County Regional Auto Theft Task Force	4
San Diego Harbor Police	11
San Diego Sheriff's Office	99
San Diego Community College District Police	1
San Diego State University Police	2
University of California, San Diego Police	7
Whittier Police	3

SEARCHES CONDUCTED BY SDPD UPON REQUEST OF OUT-OF-STATE AGENCIES

Out-of-State Agency	Times Shared
Portsmouth Police (New Hampshire)	2

SEARCHES CONDUCTED BY SDPD UPON REQUEST OF FEDERAL OR INTERNATIONAL AGENCIES

Federal/International Agency	Times Shared
Drug Enforcement Agency	20
Federal Bureau of Investigation	3
High Intensity Drug Trafficking Areas	1
Homeland Security Investigations*	4
Internet Crimes Against Children	3
Narcotics Task Force	60
U.S. Customs and Border Protection*	6
U.S. Marshals Office	3
U.S Probation	4
U.S. Secret Service	14
United States Postal Inspection Service	8
Violent Crimes Task Force	1
Royal Canadian Mounted Police	1
San Diego Human Trafficking Task Force	3
Violent Crimes Task Force	1

*These searches were not for immigration-related cases.

ADDENDUM B – EXPANDED METRICS AND CASE ILLUSTRATIONS

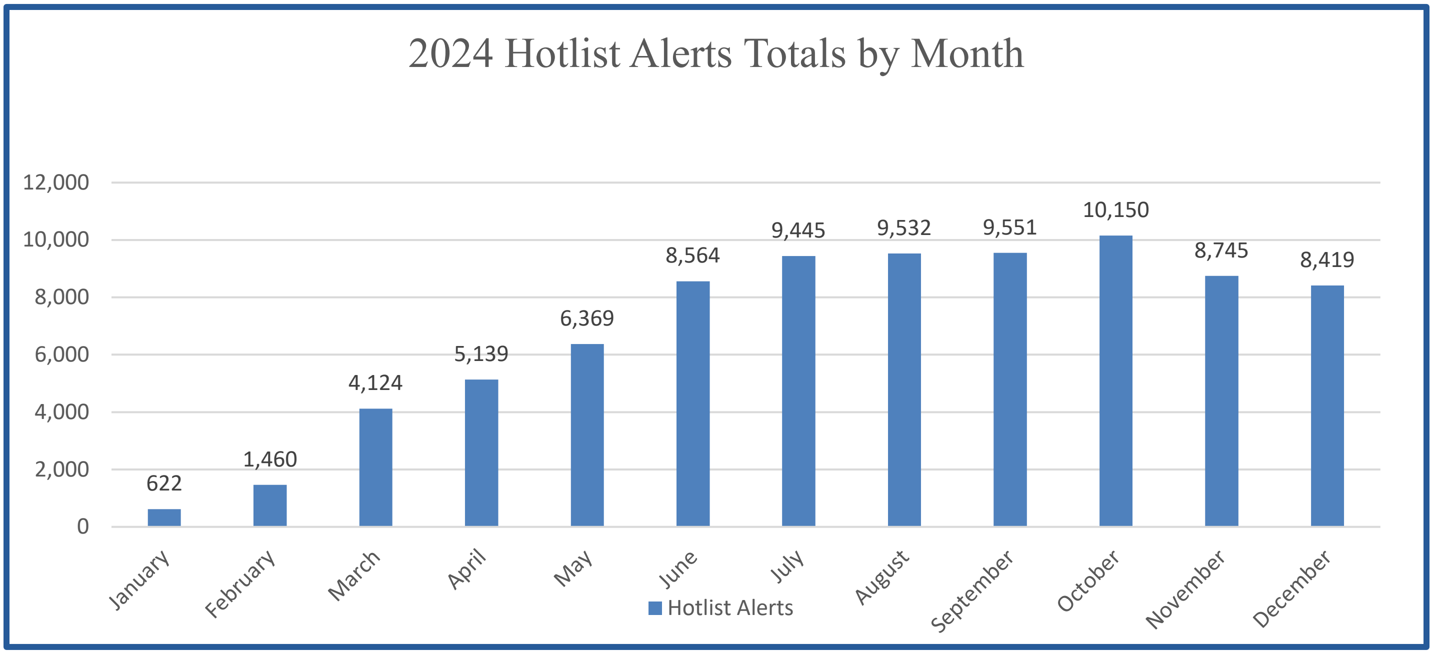
This addendum provides additional performance metrics and detailed case examples to further demonstrate the effectiveness of the Automated License Plate Reader (ALPR) system.

2024 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, the San Diego Police Department 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 2024 Hotlist Alert Chart in this report 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.



81,909	*250*	*82,159*
2024 Official Hotlist Alerts	**2024 Custom Hotlist Alerts**	**2024 Total Hotlist Alerts**

77,877	*4005*	*250*	*30*
2024 Stolen License Plate Alerts	**2024 Stolen Vehicle Alerts**	**2024 Custom Hotlist Alerts**	**2024 Felony Vehicle Alerts**

JANUARY 2024

615	*7*	*622*
Official Hotlist Alerts	**Custom Hotlist Alerts**	**Total Hotlist Alerts**

January Investigation Highlights

459 PC – Burglary

A Special Projects and Legislative Affairs (SPLA) officer used the ALPR system to follow up on a detective's Be on the Look Out (BOLO) bulletin related to a burglary in Northeastern Division. The bulletin included photos of three suspects and a 2005 Ford Expedition believed to be involved.

Using the ALPR system, the SPLA officer located recent scans of the Expedition traveling on Logan Avenue and shared this information with the assigned detective and Central Division's Crime Suppression Team (CST).

On January 11, 2024, Central CST officers located the vehicle in Logan Heights and conducted a traffic stop. Two suspects from the BOLO were inside. A consent search of the vehicle revealed more than $2,000 in stolen property from the burglary. One suspect provided a statement implicating himself and others in the crime. The vehicle was impounded, and the stolen property was returned to its owner.

211 & 538 PC – Robbery and Impersonating a Police Officer

On January 16, 2024, a victim in South Bay reported being robbed by a suspect driving a newer white Jeep Grand Cherokee equipped with red and blue emergency lights. Believing the suspect to be an officer, the victim pulled over. The suspect approached with a gun, demanded the victim's phone and wallet, and fled.

Detectives began investigating and tracked the victim's stolen phone to an area where they located a matching Jeep. The victim reported having visited the Cheesecake Factory at Fashion Valley Mall shortly before the robbery. With permission, detectives accessed the mall's private ALPR system and confirmed the suspect vehicle had been at the mall during the same timeframe as the victim.

Mall surveillance footage showed the driver illuminated by red dashboard lighting, matching the robbery description. Detectives later obtained a search warrant for the Jeep, discovering forward-facing red and blue lights and a jacket matching the suspect's clothing.

The suspect was arrested and convicted of robbery, conspiracy, and impersonating a police officer, receiving a sentence of 365 days in custody and 3 years of probation.

FEBRUARY 2024

1,447	*13*	*1,460*
Official Hotlist Alerts	**Custom Hotlist Alerts**	**Total Hotlist Alerts**

February Investigation Highlight

487 PC – Grand Theft

On February 20, 2024, Northern Division officers requested a Hotlist entry for a suspect vehicle connected to a felony theft case in Eastern Division. The vehicle, wanted under Penal Code 487 (Grand Theft), was entered into San Diego's Hotlist along with a Declaration for Arrest.

Within hours, the ALPR system generated a real-time alert. Officers immediately responded to the area, located the vehicle, and arrested the suspect without incident. A search of the vehicle led to the recovery of approximately $1,200 in stolen property, which was returned to its rightful owner.

4,118	*6*	*4,124*
Official Hotlist Alerts	**Custom Hotlist Alerts**	**Total Hotlist Alerts**

MARCH 2024

March Investigation Highlights

Missing Person – Silver Alert

On March 7, 2024, family members reported an elderly man with dementia missing after he failed to return home from the bank the previous evening. He was last seen driving a 2013 Nissan Versa from his home in Tierrasanta.

The Missing Persons Unit immediately began investigating and, working with the Special Projects and Legislative Affairs Unit, entered the vehicle's license plate into SDPD's ALPR Hotlist. This ensured SDPD would receive a real-time alert if his vehicle was detected by the City's ALPR network. A statewide Silver Alert was also issued through CHP.

At 8:47 p.m., an ALPR camera detected the vehicle on Genesee Avenue, providing officers with the location in real time. Northern Division officers quickly responded and located the man driving near Clairemont Mesa Boulevard. He was found tired and disoriented but safe.

207 & 215 PC – Kidnapping and Carjacking

On March 14, 2024, ALPR cameras detected a stolen Lexus SUV entering the Las Americas Mall in Southern

Division. A record check revealed that the vehicle had been involved in a carjacking and kidnapping in Central Division four days earlier.

Southern Division officers and detectives immediately responded, locating the vehicle unoccupied in the mall parking lot. Surveillance footage provided images of the suspects, and undercover detectives located them walking inside the mall. As the suspects returned to the stolen vehicle, officers safely took three males into custody. Two additional suspects were detained inside the mall.

The coordinated response, prompted by an ALPR alert, led to the swift arrest of five suspects and the recovery of the stolen vehicle, preventing further potential violence.

459 PC – Burglary

On March 8, 2024, two suspects broke into Mr. Shawarma's Restaurant on Garnet Avenue. Surveillance footage showed the same individuals near the business days earlier, apparently casing the location. Both incidents involved a black Volkswagen sedan with temporary paper plates, making identification difficult. A Northern Division Crime Suppression Team officer used the ALPR system to search for the vehicle and obtained a clear image that revealed the full license plate number. Investigators used that information to identify and charge the two suspects with burglary.

APRIL 2024

5,107	*32*	*5,139*
Official Hotlist Alerts	**Custom Hotlist Alerts**	**Total Hotlist Alerts**

April Investigation Highlights

10851 CVC – Stolen Vehicle and Firearm Recovery

On April 17, 2024, Mid-City Division officers received an ALPR alert for a stolen vehicle near 3300 University Avenue. Officers quickly located the vehicle within ten minutes and conducted a felony stop, safely detaining the driver.

During a search of the vehicle, officers recovered an unserialized firearm (also known as a ghost gun) loaded with 16 rounds, a controlled substance, and various burglary tools. The driver was arrested for multiple felony violations, including possession of a stolen vehicle, possession of a firearm by a felon, possession of a controlled substance while armed, possession of an unserialized firearm, and possession of a large-capacity magazine.

10851 CVC – Stolen Vehicle and Parole Violation Arrest

On April 18, 2024, Western Division officers responded to an ALPR alert for a stolen vehicle parked at Fashion Valley Mall. The vehicle was occupied by two males, one of whom was known to have two active felony warrants.

As officers approached, the driver fled on foot but was quickly apprehended and arrested for possession of a stolen vehicle and his outstanding warrants. The passenger, who remained in the car, was found with a white drawstring bag containing 46 rounds of .38 Special ammunition. A records check showed he was on active parole, leading to his arrest for parole a violation and being a felon in possession of ammunition.

MAY 2024

6,357	12	6,369
Official Hotlist Alerts	**Custom Hotlist Alerts**	**Total Hotlist Alerts**

May Investigation Highlights

243(d) PC – Felony Battery (Serious Injury)

On March 20, 2024, a victim filed a report at the Eastern Division front counter after being attacked by a coworker, suffering a broken jaw. The victim provided the suspect's vehicle license plate number to investigators.

On May 3, 2024, officers received an ALPR alert for a vehicle linked to a wanted felony suspect near 5390 Balboa Avenue. With assistance from ABLE (the police helicopter), officers located the vehicle in the Costco parking lot on Morena Boulevard. The driver was identified as the suspect in the felony battery case and was arrested without incident. He was transported to Eastern Division for an interview with the assigned detective.

459 PC – Burglary

A Special Projects and Legislative Affairs (SPLA) officer proactively followed up on a detective's "Be On the Lookout" (BOLO) bulletin related to a burglary in Northern Division. The bulletin included a photo of the suspect vehicle used in the crime.

Using the ALPR system, the SPLA officer conducted a records search and successfully identified the vehicle. The information was shared with the assigned detective, providing a crucial lead in the investigation.

211 PC – Attempted Bank Robbery (2023 Case)

The Robbery Unit requested assistance from the SPLA Unit to identify a suspect vehicle involved in a 2023 attempted bank robbery. Investigators provided an image of a small black SUV with paper plates and an aftermarket trailer hitch.

An SPLA detective used the ALPR system to locate a similar vehicle with a temporary DMV permit and matching features. On May 9, 2024, officers located the vehicle in Northern Division and conducted surveillance. About 20 minutes later, a male entered the vehicle. Officers confirmed he matched the BOLO photo of the robbery suspect and took him into custody.

The suspect was arrested for the attempted bank robbery and an outstanding warrant.

JUNE 2024

8,562	*2*	*8,564*
Official Hotlist Alerts	**Custom Hotlist Alerts**	**Total Hotlist Alerts**

June Investigation Highlights

211 PC – Robbery

On June 11, 2024, the SDPD Robbery Unit requested assistance from the Special Projects and Legislative Affairs (SPLA) Unit to help identify a suspect vehicle connected to a robbery that occurred on May 12, 2024.

An SPLA detective used the ALPR system to conduct a records search and successfully identified the vehicle involved. The detective provided the results to the assigned Robbery Unit investigator, generating a key lead that advanced the ongoing investigation.

664/207 PC – Attempted Kidnapping

On June 20, 2024, an Eastern Division detective requested that a suspect vehicle in an attempted kidnapping of a six-year-old be entered into SDPD’s ALPR Hotlist, allowing Citywide alerts if the vehicle appeared on camera.

At 3:45 p.m. that same day, the ALPR system detected the vehicle in downtown San Diego, prompting an immediate patrol response. Within minutes, Central Division officers located the vehicle and detained the suspect. He was arrested for the June 18, 2024, attempted kidnapping in the Mission Valley area.
A total of 24 investigators conducted 237 ALPR searches throughout the investigation, reflecting SDPD’ coordinated, data-driven effort to locate the suspect quickly.

211 PC – Robbery Series

Northeastern Division officers received an ALPR alert for a felony vehicle wanted in connection with a series of robberies in Escondido. Officers located the vehicle near 6800 Miramar Road, conducted a high-risk stop, and safely detained the driver.

An Escondido Police Department detective investigating the robbery series responded, took custody of the suspect, and impounded the vehicle as evidence.

JULY 2024

9,439	*6*	*9,445*
Official Hotlist Alerts	**Custom Hotlist Alerts**	**Total Hotlist Alerts**

July Investigation Highlights

211 PC – Armed Robbery Series

On July 10, 2024, the San Diego Police Department Robbery Unit requested assistance from the Special

Projects and Legislative Affairs (SPLA) Unit to identify a suspect vehicle connected to four armed robberies that occurred overnight in the San Diego and El Cajon areas.

An SPLA detective used the ALPR system to conduct searches and successfully identified the suspect vehicle. The results were provided to the Robbery Unit, giving detectives a key investigative lead.

Evidence gathered through the ALPR system ultimately allowed detectives to identify, locate, and arrest the suspect responsible for the armed robbery series. The suspect was later convicted and sentenced to four years in prison.

288 PC – Lewd Acts with a Minor

Between 1:50 a.m. and 4:50 a.m. on July 18, 2024, a female juvenile under 14 years old was sexually assaulted by an unknown suspect inside his vehicle at the College Grove Center parking lot. The vehicle was described as an older Chevrolet Cruze sedan with a temporary tag displayed in the rear windshield.

A Special Projects and Legislative Affairs (SPLA) detective reviewed ALPR images and Smart Streetlight video to confirm that the suspect's vehicle had been present at the location during the time of the assault, corroborating the victim's account and providing critical evidence for investigators.

On July 19, 2024, the suspect was arrested on multiple sexual assault charges involving a minor, and his vehicle was impounded as evidence. He was later convicted and sentenced to five years in prison.

AUGUST 2024

9,506	*26*	*9,532*
Official Hotlist Alerts	**Custom Hotlist Alerts**	**Total Hotlist Alerts**

August Investigation Highlights

422.6 PC – Hate Crime

On August 2, 2024, unknown suspects vandalized a bar in the 3700 block of Fifth Avenue, spray-painting swastikas and derogatory slurs on a wall and trash can. Witnesses reported that the suspects briefly returned to the scene in a late 1990s or early 2000s Buick Century with a missing front passenger hubcap before fleeing.

On August 3, 2024, a Special Projects and Legislative Affairs (SPLA) detective was contacted to assist in identifying the vehicle. Using the ALPR system, the detective conducted multiple searches and was able to positively identify the suspect vehicle and confirm that it had been in the immediate area of the crime scene.

The information was provided to the case agent, who later identified and arrested the suspects.

211 PC – Robbery Series

On August 5, 2024, a suspect committed two armed robberies within hours along El Cajon Boulevard, targeting an Advance America Cash Advance and Discount Liquor. In both incidents, the suspect brandished a black semi-automatic handgun, demanded money, and fled with cash totaling approximately $700.

Robbery detectives reviewed surveillance footage and identified the suspect entering a red Nissan sedan shortly after one of the robberies. A Mid-City patrol officer used the ALPR system to review nearby camera data and positively identified the vehicle, forwarding the information to detectives.
On August 8, 2024, detectives located and arrested the suspect, recovering a loaded Springfield XD handgun with live ammunition during a search of his residence. The suspect was booked into San Diego Central Jail for 211 PC – Robbery.

209 PC, 261 PC & 236 PC – Kidnapping, Rape, and False Imprisonment

On August 17, 2024, a victim accepted a ride from a suspect who later sexually assaulted and imprisoned her. The victim managed to escape and provided detectives with a detailed description of the suspect and his vehicle.

On August 19, 2024, investigators used ALPR data to identify the suspect's vehicle and place it near the scene during the time of the assault. Follow-up checks confirmed the vehicle's registered owner, and the victim positively identified the suspect in a lineup.

The Special Investigations Unit located the suspect and arrested him on multiple felony charges, including rape, kidnapping, and false imprisonment. He was later convicted.

SEPTEMBER 2024

9,531	*20*	*9,551*
Official Hotlist Alerts	**Custom Hotlist Alerts**	**Total Hotlist Alerts**

September Investigation Highlights

211 PC – Robbery

On September 1, 2024, a smoke shop in Northeastern Division was robbed at gunpoint. The suspects fled with stolen property and were picked up by a getaway driver in a vehicle with an unknown license plate. Surveillance video captured both the suspects and the waiting vehicle, but the license plate was unreadable.

Although Robbery Unit detectives were able to identify the suspects from the surveillance footage, they were initially unable to confirm the getaway vehicle. On September 10, 2024, the case agent requested assistance from the Special Projects and Legislative Affairs (SPLA) Unit.
Using ALPR and Smart Streetlight camera data, an SPLA detective conducted an investigative follow-up and positively identified the suspect vehicle. The suspect was later arrested and convicted.

245 PC – Assault with a Deadly Weapon

On September 28, 2024, SDPD Communications received a report that a suspect had assaulted and run over a victim with a vehicle before fleeing the scene.

The SPLA Unit reviewed Smart Streetlight video from the area and found that the entire incident had been captured on camera, providing investigators with clear details of the suspect vehicle. Using this footage, detectives conducted targeted ALPR searches, which positively identified the vehicle.

Patrol officers immediately saturated the area where the suspect vehicle was last detected and successfully located and arrested the driver. Detectives responded to conduct a follow-up investigation.

OCTOBER 2024

10,150	*39*	*10,189*
Official Hotlist Alerts	**Custom Hotlist Alerts**	**Total Hotlist Alerts**

October Investigation Highlights

288 PC & 261 PC – Lewd Acts with a Minor and Rape

On October 9, 2024, a Child Abuse Unit detective requested assistance from the Special Projects and Legislative Affairs (SPLA) Unit in locating a suspect wanted for rape and child molestation involving multiple victims.

Using investigative details provided by the case detective, an SPLA detective searched the ALPR database and positively identified the suspect's vehicle. The vehicle was then added to SDPD's ALPR Hotlist to generate real-time alerts if detected.

Later that evening, an ALPR camera in Mid-City Division detected the suspect vehicle. Detectives responded, located the car parked and unoccupied, and maintained surveillance. In the early morning hours of October 10, 2024, the suspect returned to the vehicle and was taken into custody without incident. A firearm was recovered from the suspect at the time of arrest.

207 PC – Kidnapping

On October 5, 2024, a suspect and accomplice kidnapped a victim at knifepoint, forcing the victim into their vehicle. A witness immediately called 911 and provided detailed information about the suspect's vehicle.

Western Division patrol officers used the ALPR system to identify recent detections of the vehicle and responded to the area. Officers quickly located the suspect vehicle and conducted a high-risk traffic stop, taking both suspects into custody. The victim was found safe inside the vehicle, and the knife used in the crime was recovered.

The Domestic Violence Unit responded to continue the investigation, and Smart Streetlight video footage captured the entire incident, providing critical supporting evidence.

NOVEMBER 2024

8,689	*56*	*8,745*
Official Hotlist Alerts	**Custom Hotlist Alerts**	**Total Hotlist Alerts**

DECEMBER 2024

8,388	*31*	*8,419*

Official Hotlist Alerts	Custom Hotlist Alerts	Total Hotlist Alerts

December Investigation Highlights

459 PC – Burglary

On November 19, 2024, at approximately 3:00 a.m., two businesses in the Tierrasanta community were burglarized. Surveillance video captured a gray sedan involved in the crime, but the license plate was partially obscured. Using Automated License Plate Reader (ALPR) data, detectives were able to identify a potential vehicle and license plate connected to the burglaries.

On November 25, 2024, the same vehicle returned to Tierrasanta and was involved in two additional business burglaries, confirming it as the suspect vehicle. Detectives shared the vehicle and suspect information with patrol officers Citywide.

On December 12, 2024, two more burglaries occurred in the 4S Ranch and University City areas. Although limited suspect information was available, officers used ALPR data from the prior investigation and discovered the suspect vehicle had been detected nearby. Patrol units saturated the area, located the vehicle near Interstate 5 and State Route 56, and arrested the suspect without incident.

Throughout this multi-jurisdictional investigation, officers conducted over 3,000 ALPR searches to gather evidence, connect related cases, and locate the suspect.

San Diego Police Department

Body Worn Camera (BWC)

Department/Division: Police - Logistics

Related Policy/Procedure:

- DP 1.49 – Body Worn Cameras

DESCRIPTION

Body Worn Cameras (BWCs) are a vital tool in improving and enhancing the safety of officer and civilian interactions. BWC are used to capture audio and visual evidence for investigations and enforcement encounters. 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.

During 2024, San Diego Police Department officers recorded 750,265 body worn camera videos.

SHARING OF DATA

Approximately 20,000 “CASES” were created in Evidence.com in 2024 by investigators for the purpose of sharing BWC videos with the San Diego District Attorney’s Office and City Attorney’s Office. The “CASES” feature in Evidence.com allows investigators to organize all BWC videos in a specific folder. Those folders are then shared through the secured Axon Evidence.com website with the prosecutorial agency. Approximately 9,032 CASES were shared with the District Attorney’s Office. 10 CASES were also shared with the Riverside District Attorney’s Office 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	2
Coronado Police	3
Chula Vista Police	10
Harbor Police	2
El Cajon Police	2
Oceanside Police	1
National City Police	7

Additionally, in accordance with Senate Bill 1421/16, “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 law defines the scope of disclosable records. The BWC videos related to the “specified incidents” are redacted and posted on the City of San Diego’s website at www.sandiego.gov.

The San Diego Police Department (SDPD) receives subpoenas for BWC videos regarding civil litigation. In compliance with civil law and or court order, the BWC videos are shared through Evidence.com. In 2024, SDPD complied with approximately 280 civil subpoenas.

Four “CASES” in Evidence.com were shared with the California Commission on Peace Officer Standards and Training (POST). The CASES were shared to California POST for investigations regarding use of force incidents in compliance with state law.

LOCATION

SDPD’s sworn personnel wear the BWC on their midsection on their outermost item of clothing and utilize their viewers to ensure the BWC is in a position where the field of view provides for effective recording.

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 4 Body 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 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 and has not received any reports of disproportionate impacts. The Use Policy continues to protect civil rights and civil liberties.

AUDITS OR INVESTIGATIONS

Per SDPD Department Procedure 1.49 and OR 24-16, Supervisory Responsibilities for BWC Inspection, 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."

Evidence.com will display the BWC videos assigned to the officer. Supervisors shall notify the officer of the videos that have not been labeled and ensure the officer inputs the correct event number so the video can be accessed easily by investigators. The Supervisor will reinspect the videos assigned to the officer to ensure all BWC videos have been labeled correctly.

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.

DATA BREACH OR UNAUTHORIZED ACCESS

SDPD is not aware of any data breaches or unauthorized access to the data collected by this 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 two factors 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.

Additionally, 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 SDPD's 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. 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.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

There were 176 California Public Records Act requests referencing this technology in 2024.

Request Number	Opened Date	Closed Date
24-432	01/19/2024	01/29/2024
24-4445	06/27/2024	07/05/2024
24-1088	02/13/2024	02/23/2024
24-3219	05/09/2024	05/17/2024
24-8538	12/09/2024	12/19/2024
24-8454	12/04/2024	12/13/2024
24-3770	05/31/2024	06/10/2024
24-848	01/31/2024	02/09/2024
24-1161	02/16/2024	02/26/2024
24-1142	02/15/2024	02/23/2024
24-3716	05/30/2024	06/07/2024
24-7222	10/16/2024	10/31/2024
24-3653	05/28/2024	06/07/2024
24-5175	07/30/2024	08/09/2024
24-2669	04/16/2024	04/26/2024
24-1185	02/18/2024	03/01/2024
24-2048	03/21/2024	04/12/2024
24-8400	12/03/2024	12/13/2024
24-2047	03/21/2024	04/12/2024
24-8155	11/21/2024	11/29/2024
24-1442	02/26/2024	03/07/2024

Request Number (continued)	Opened Date	Closed Date
24-6155	09/07/2024	09/19/2024
24-6487	09/19/2024	09/27/2024
24-3849	06/04/2024	06/14/2024
24-4152	06/14/2024	06/24/2024
24-4193	06/17/2024	06/27/2024
24-3718	05/30/2024	06/07/2024
24-6273	09/11/2024	09/20/2024
24-5625	08/16/2024	08/26/2024
24-5630	08/16/2024	08/26/2024
24-4960	07/22/2024	08/01/2024
24-4041	06/11/2024	06/21/2024
24-7422	10/23/2024	11/01/2024
24-2685	04/16/2024	04/26/2024
24-7235	10/17/2024	10/25/2024
24-4890	07/18/2024	07/26/2024
24-4067	06/12/2024	06/21/2024
24-356	01/16/2024	01/26/2024
24-1443	02/26/2024	03/07/2024
24-6340	09/14/2024	09/26/2024
24-4310	06/21/2024	07/05/2024
24-8316	11/27/2024	12/06/2024
24-6694	09/26/2024	10/04/2024
24-4692	07/10/2024	07/19/2024
24-7032	10/09/2024	10/18/2024
24-5376	08/07/2024	08/16/2024
24-8340	12/01/2024	12/12/2024
24-3344	05/14/2024	05/24/2024
24-3690	05/29/2024	06/07/2024
24-7662	11/02/2024	11/14/2024
24-1079	02/19/2024	02/23/2024
24-3613	05/24/2024	06/03/2024
24-4687	07/09/2024	07/19/2024
24-7423	10/23/2024	11/01/2024
24-4212	06/17/2024	06/27/2024
24-2988	05/01/2024	05/10/2024
24-5843	08/26/2024	09/05/2024
24-3822	06/03/2024	06/13/2024
24-5668	08/19/2024	09/03/2024
24-5164	07/30/2024	08/09/2024
24-5293	08/04/2024	08/15/2024
24-2460	04/08/2024	04/18/2024
24-3380	05/15/2024	05/24/2024
24-3987	06/10/2024	06/20/2024
24-4456	06/27/2024	07/05/2024
24-4795	07/15/2024	07/25/2024
24-4648	07/09/2024	07/19/2024
24-4972	07/22/2024	08/15/2024
24-4731	07/11/2024	07/19/2024

Request Number (continued)	Opened Date	Closed Date
24-3717	05/30/2024	06/07/2024
24-1568	02/19/2024	03/08/2024
24-4917	07/18/2024	07/26/2024
24-8830	12/19/2024	12/27/2024
24-5091	07/26/2024	08/05/2024
24-3578	05/23/2024	05/31/2024
24-1686	03/06/2024	03/15/2024
24-4654	07/08/2024	07/18/2024
24-3398	05/15/2024	05/24/2024
24-5638	08/17/2024	08/29/2024
24-6170	09/08/2024	09/19/2024
24-7137	10/14/2024	10/24/2024
24-7424	10/23/2024	11/01/2024
24-1078	02/13/2024	02/23/2024
24-3272	05/10/2024	05/20/2024
24-5400	08/08/2024	08/16/2024
24-3163	05/07/2024	05/17/2024
24-6640	09/25/2024	10/04/2024
24-7205	10/16/2024	10/25/2024
24-715	01/30/2024	02/09/2024
24-6866	10/04/2024	10/14/2024
24-396	01/18/2024	01/26/2024
24-1156	02/16/2024	02/26/2024
24-2852	04/23/2024	05/03/2024
24-2305	04/02/2024	04/12/2024
24-3380	05/15/2024	05/24/2024
24-3987	06/10/2024	06/20/2024
24-4456	06/27/2024	07/05/2024
24-4795	07/15/2024	07/25/2024
24-4684	07/09/2024	07/19/2024
24-4972	07/22/2024	08/15/2024
24-4731	07/11/2024	07/19/2024
24-3717	05/30/2024	06/07/2024
24-1568	02/29/2024	03/08/2024
24-4917	07/18/2024	07/26/2024
24-8830	12/19/2024	12/27/2024
24-5091	07/26/2024	08/05/2024
24-3578	05/23/2024	05/31/2024
24-1686	03/06/2024	03/15/2024
24-4654	07/08/2024	07/18/2024
24-3398	05/15/2024	05/24/2024
24-7334	10/22/2024	11/01/2024
24-8521	12/07/2024	12/19/2024
24-4116	06/12/2024	06/21/2024
24-6023	09/02/2024	09/13/2024
24-6314	09/13/2024	09/23/2024
24-6251	09/11/2024	09/20/2024
24-1385	02/22/2024	03/01/2024

Request Number (continued)	Opened Date	Closed Date
24-6138	09/06/2024	09/16/2024
24-8552	12/09/2024	01/24/2025
24-7662	11/02/2024	11/14/2024
24-4106	06/12/2024	06/21/2024
24-8863	12/22/2024	01/02/2025
24-7510	10/27/2024	11/15/2024
24-8618	12/11/2024	12/20/2024
24-4114	06/12/2024	06/21/2024
24-4663	07/09/2024	07/19/2024
24-6861	10/04/2024	10/14/2024
24-8323	11/27/2024	12/06/2024
24-7557	10/29/2024	11/08/2024
24-3947	06/07/2024	06/18/2024
24-6458	09/18/2024	09/27/2024
24-6178	09/09/2024	09/19/2024
24-6073	09/04/2024	09/13/2024
24-125	01/06/2024	01/18/2024
24-7513	10/27/2024	11/07/2024
24-820	02/03/2024	02/15/2024
24-6763	10/01/2024	Still Open
24-1078	02/13/2024	02/23/2024
24-5956	08/29/2024	09/06/2024
24-8654	12/12/2024	12/20/2024
24-8170	11/22/2024	12/02/2024
24-6222	09/10/2024	09/20/2024
24-6985	10/08/2024	10/18/2024
24-5703	08/20/2024	08/30/2024
24-8961	12/30/2024	01/09/2025
24-8707	12/14/2024	12/26/2024
24-8710	12/14/2024	12/26/2024
24-8709	12/14/2024	12/26/2024
24-3690	05/29/2024	06/07/2024
24-8713	12/14/2024	12/26/2024
24-6958	10/07/2024	10/17/2024
24-8711	12/14/2024	12/24/2024
24-7361	10/22/2024	11/01/2024
24-8708	12/14/2024	12/26/2024
24-8705	12/14/2024	12/31/2024
24-5017	07/23/2024	08/02/2024
24-8720	12/15/2024	12/26/2024
24-8721	12/15/2024	12/26/2024
24-5801	08/23/2024	09/13/2024
24-7556	10/29/2024	11/08/2024
24-122	01/05/2024	01/12/2024
24-2216	03/28/2024	04/05/2024
24-7784	11/06/2024	11/29/2024
24-8706	12/14/2024	12/26/2024
24-3784	05/31/2024	06/10/2024

Request Number (continued)	Opened Date	Closed Date
24-7783	11/06/2024	11/29/2024
24-8704	12/14/2024	12/26/2024
24-8717	12/14/2024	12/26/2024
24-1039	02/12/2024	03/07/2024
24-8712	12/14/2024	12/26/2024
24-8872	12/23/2024	01/16/2025
24-4477	06/28/2024	07/08/2024
24-1888	03/14/2024	03/22/2024
24-4105	06/12/2024	07/02/2024
24-2691	04/16/2024	Still Open
24-7954	11/14/2024	Still Open

ANNUAL COST

The cost for FY 2024 is $1,145,248.49. For FY 2025 the cost is estimated at $2,157,618.99. This cost is funded through the state COPS fund.

REQUESTED MODIFICATIONS TO THE USE POLICY

The following modifications to the Axon Body Worn Camera Use Policy are proposed.

- Replace title to "Body Worn Camera System."
- Remove mention of "Axon Body 3" or other Axon hardware and make the terms more general.
    - This change allows for newer versions of the BWCs, as long as no updates or changes to the technology occur. Any such substantive changes would require a review through the TRUST Ordinance process.

San Diego Police Department

Smart Streetlights (SSL)

Department/Division: Police - Special Project and Legislative Affairs

Related Policy/Procedure:

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

DESCRIPTION

The San Diego Police Department used video evidence, along with data and information from authorized technologies embedded within Smart Streetlights (SSL) over 1,400 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 clear understanding to how events unfolded.

SHARING OF DATA

In addition to SDPD personnel providing video evidence and data to the District 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 video evidence and data were shared to other law enforcement agencies:

Agency Shared With	Crime
California Highway Patrol (CHP)	187 PC – Homicide
California Highway Patrol (CHP)	Urgent Officer Cover Request
California Highway Patrol (CHP)	187 PC - Homicide

LOCATION

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

UPDATES, UPGRADES, AND CONFIGURATION CHANGES

There were no upgrades or configuration changes that altered the functionality of this technology or the scope of use or deployment on the technology.

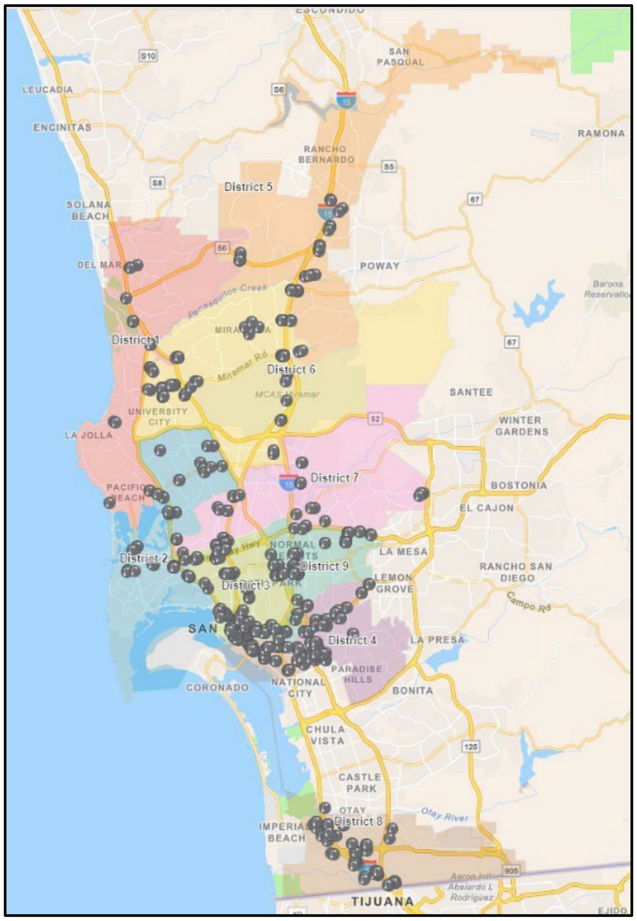
DEPLOYMENT LOCATION

The Smart Streetlights with embedded ALPR technology were deployed citywide in all police divisions.

Table 1 – Shows the City of San Diego Council District Map with current Smart Streetlights. For further detail, open attached hyperlink.

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

TABLE 1



COMMUNITY COMPLAINTS OR CONCERNS

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. Other than a letter dated July 31, 2024, from the Community Advocates for Just and Moral Governance titled "Notice of Violations of the TRUST Ordinance – Smart Streetlights and Automated License Plate Readers," 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

A supervisor of the Special Projects and Legislative Affairs Unit conducted weekly audits of the system. Any identified discrepancies with metadata entry were immediately addressed with the user.

- All documentation provided to officers regarding improper use of the system is considered a personnel record and not subject to disclosure per California Penal Code section 832.7 and California Evidence Code section 1043 (peace officer personnel records).

DATA BREACH OR UNAUTHORIZED ACCESS

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

DATA BREACH DETECTION

The City's Department of Information Technology (IT) 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

Department Procedure 3.33 mandates that videos collected by Smart Streetlights shall be stored in a secured law enforcement facility with multiple layers of physical security and security protection.

Encryption, firewalls, authentication, and other reasonable security measures were utilized to protect digital evidence from Smart Streetlights.

All Smart Streetlights videos downloaded from a video management solution to a mobile workstation or to digital evidence storage like Axon evidence were accessible only through a login/password-protected system capable of documenting all access of information by name, date and time. Only those employees of the San Diego Police Department working in an investigative or enforcement function and authorized by the Chief of Police shall access Smart Streetlights videos.

INFORMATION AND STATISTICS

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.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

There were 12 Public Records Act requests regarding SSL.

Request Number	Request Date	Closed Date
24-2164	03/26/2024	04/05/2024
24-2397	4/5/2024	05/22/2024
24-2407	4/5/2024	04/10/2024
24-2735	4/18/2024	04/21/2024
24-3257	5/10/2024	05/21/2024
24-5942	8/28/2024	09/01/2024
24-6390	9/17/2024	09/20/2024
24-6912	10/6/2024	10/20/2024
24-7240	10/17/2024	10/21/2024
24-7535	10/28/2024	11/05/2024
24-8378	12/2/2024	12/07/2024
24-8608	12/10/2024	12/14/2024

ANNUAL COST

On 12-26-2023 an initial payment of $3,512,500 was paid for installation and one (1) year of service for the 500 Smart Streetlights with embedded Automated License Plate Recognition technology.

On 6-24-2024 a payment of $6,800 was disbursed for relocation of SSL/ALPR units.

On 12-11-2024 a payment of $1,449,602.08 was authorized for calendar year 2025 contract obligations.

All funding sources were from the city general fund.

REQUESTED MODIFICATIONS TO THE USE POLICY

The following modifications to the Smart Streetlight Use Policy are proposed:

- 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 typo and language corrections. These corrections do not have any impact on the use of the technology.

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 robots that are used by the San Diego Police Department (SDPD) Special Weapons and Tactics (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.

For the 2024 calendar year, the San Diego Police Department 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 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 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.

SHARING OF DATA

Data collection, Data Access, Data Protection, Data Retention, Public Access, and Third Party Data Sharing for all robot platforms is listed in the Surveillance Use Policies. No data from these robots was shared with third parties.

LOCATION

The robots are used by the SWAT unit exclusively personnel and housed in the Special Equipment Vehicle or SDPD Headquarters 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.

UPDATES, UPGRADES, AND CONFIGURATION CHANGES

The ICOR robot received a hardware update that enables the SWAT Unit to deploy chemical agents into a structure or area remotely. This capability is not permanently affixed to the robot and is only used in specific circumstances. There were no other changes to the robot due to this hardware addition.

The ICOR robot was also sent back to the manufacturer for routine maintenance on consumable parts due to damage sustained during a SWAT incident. There were no upgrades or changes to the operation of the robot. The FirstLook (Gen 2) was sent back to the manufacturer for routine maintenance on consumable parts. There were no upgrades or changes to the operation of the robot.

DEPLOYMENT LOCATION

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 approximately 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
NORTHERN DIVISION (100S)	3
NORTHEASTERN DIVISION (200S)	1
EASTERN DIVISION (300S)	2
SOUTHEASTERN DIVISION (400s)	7
CENTRAL DIVISION (500s)	2
WESTERN DIVISION (600s)	1
SOUTHERN DIVISION (700s)	4
MID-CITY DIVISION (800s)	6
NORTHWESTERN DIVISION (900s)	2
OUT OF CITY (BEAT 999)	8

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

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

DATA BREACH OR UNAUTHORIZED ACCESS

The Department is not aware of data breaches or unauthorized access to the data collected by this 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, 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.

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.

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.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

There were no California Public Records Act requests regarding this technology.

ANNUAL COST

In 2024, 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.

REQUESTED MODIFICATIONS TO THE USE POLICY

The SDPD requests a modification to this technology’s Use Policy to include that the First Look II robot would also be utilized by the Special Operations Unit (SOU). Only SWAT, or SOU supervisors after being trained, could authorize the deployment of the First Look II robot. The First Look II robot would still be operated by SWAT personnel exclusively.

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

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 cameras, this technology provides a video image of a space that would be either unable to be seen with the human eye using infrared technology or would be too dangerous to place a human in. Through the use of a microphone on the robot, it is able to provide the user with live audio of the space that it is in.

This technology was deployed twice in 2024.

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 portable unit that is not installed anywhere specifically. The robot 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 2024. Both instances were in the Southeastern Division police service area.

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

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

DATA BREACH OR UNAUTHORIZED ACCESS

SDPD is not aware of any data breaches or unauthorized access to the data collected by this 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, 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

This technology was deployed twice in 2024.

One of those deployments allowed the SDPD SWAT units to check under a door during a mission, to clear the bathroom for potential safety hazards. The camera identified two dogs that were unleashed in the bathroom, thus preventing harm to the officers or the dogs.

This technology was also deployed to visually clear a room, which prevented SWAT officers from having to enter the room if a suspect was present, potentially preventing loss of life and critical time from being diverted in the event.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

There were no Public Records Act requests regarding this technology.

ANNUAL COST

In 2024, SDPD did not expend any funds for this technology and does not have any projected costs in 2025 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

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 approximately 40 times in 2024. There were 13 arrests made using this technology which were forwarded to the DA's Office.

SHARING OF DATA

In 2024, data, in the form of written testimony 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 bike being valued at over $950. 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.

13 cases were sent to the District Attorney's Office for prosecution.

LOCATION

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 surveillance technology operates in the San Diego Police Northern Division area (100 Service Area).

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 and has not received any reports of disproportionate impacts. The Use Policy continues to protect civil rights and civil liberties.

AUDITS OR INVESTIGATIONS

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

DATA BREACH OR UNAUTHORIZED ACCESS

The SDPD is not aware of any data breaches or unauthorized access to the data collected by this 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, 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. 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.

Of the approximately 40 deployments of this technology, there were 13 arrests, and 13 cases were submitted to the DA's Office for prosecution.

CALIFORNIA PUBLIC RECORDS ACT REQUESTS

There were no Public Records Act requests regarding this technology.

ANNUAL COST

The annual fiscal cost of the software is $4,200. The funds for services and bike repairs are paid through general funds. This will continue in 2025.

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 San Diego Police Department utilizes vehicle tracking devices to track suspect vehicles involved in ongoing criminal investigations, locate wanted suspects, or locate stolen property. The vehicle trackers were utilized 28 times in 2024.

The Department utilizes object tracking devices to track suspects and locate stolen property. These trackers have not been deployed during 2024.

SHARING OF DATA

Sharing of data is at the discretion of the detective handling the investigation and is not reported back to the Robbery Unit.

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.

LOCATION

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

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 vehicle trackers were deployed in all SDPD service areas.

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.

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

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

DATA BREACH OR UNAUTHORIZED ACCESS

The Department is not aware of data breaches or unauthorized access to the data collected by this 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, 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 these technologies.

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.

CALIFORNIA PUBLIC RECORDS ACT REQUEST

There were no Public Records Act requests regarding these technologies.

ANNUAL COST

The cost for the service is $15,045.25 a year for the vehicle trackers.

The cost for the service is $1560.00 a year for the object trackers.

The funding for the vehicle and object trackers is from the Department's General Fund.

REQUESTED MODIFICATIONS TO THE USE POLICY

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

Conclusion

This Annual Surveillance Report reaffirms the SDPD’s commitment to providing open dialogue and transparency to our community members and elected officials. The surveillance equipment the SDPD employs allows officers to enhance the safety of the public, provide officers with better situational awareness, resolve critical incidents safely, and assist in criminal investigations. The SDPD continues to strive to preserve human life, partner with the community, hold ourselves to the highest standards of integrity and advance innovations within the law enforcement community.

This report encapsulates the various technologies utilized by the SDPD to protect and serve the community, in addition to ensuring compliance with the law. The SDPD continues to meet or exceed the requirements of the ordinance. The SDPD has complied with the ordinance and has demonstrated the benefits to the community of the City’s acquisition and use of the surveillance technologies outweigh the costs. The proposed use of surveillance technology will safeguard civil rights and civil liberties. Based on the facts and information presented to the City Council, there is no effective alternative to the proposed surveillance technology that provides a lesser financial cost to the City and impact on civil rights or civil liberties.

This Annual Surveillance Report has fulfilled the obligations under the Municipal Code, specifically, the Transparent and Responsible Use of Surveillance Technology ordinance. The SDPD looks forward to feedback from the Privacy Advisory Board, community stakeholders, and City Council during this process and in the future.