
# 2025 Annual Surveillance Report

## San Diego Fire-Rescue Department

## Introduction

San Diego Fire-Rescue Department's (SDFD) mission is to provide the highest quality public safety services to the communities it serves. SDFD values transparency and public input and welcomes open dialogue about its practices and operations. The preservation and sustainability of public safety, firefighter safety and civil rights is paramount. SDFD further recognizes the importance and value of public disclosure regarding the qualified surveillance technology used by SDFD.

The surveillance equipment listed in this annual report are essential and valuable tools for incident command (IC) staff to gain situational awareness on a variety of emergency responses. The use of technology assists incident command staff in deploying the appropriate number of resources to strategic locations to efficiently mitigate complex emergency incidents. Technology also provides real-time information during various fire incidents by identifying hot spots, assessing structural integrity, and the effectiveness of firefighting suppression efforts. Technology can also identify water related emergencies in areas that are not normally staffed by Lifeguard personnel. The information gathered from the surveillance equipment can be shared with land and water-based rescue units to decrease the response time to life threatening water related emergencies.

## 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.

# Unmanned Aircraft System

**Department/Division: Fire Rescue/Special Operations**

**Subject Matter Expert: Captain Jeff Ring**

**Phone Number and Extension: (619) 236-6815**

**Related Policy/Procedure:**

- SDFD Operations Manual, Standard Instruction 02, Section 46 – Unmanned Aircraft System (UAS)
- SDFD UAS Operations Manual

## DESCRIPTION

SDFD UAS were dispatched to a total of 21 incidents during calendar year 2025. The incident types included structure fires, vegetation fires, and an open space rescue. Of the 21 incident dispatches, SDFD flew the UAS on 11 of these incidents. The primary purpose of the UAS flights were to locate hot spots during active fire incidents and to confirm extinguishment. The open space rescue incident involved using thermal imagery to locate a missing hiker.

## SHARING OF DATA

Of the 11 incidents where the UAS was flown, no imagery was retained or shared outside of SDFD.

## LOCATION

The UAS is a mobile resource that is deployed to a location upon request on an as needed basis.

## UPDATES, UPGRADES, AND CONFIGURATION CHANGES

In early 2025, SDFD initiated the process of placing four new aircraft in service. The capabilities and uses of UAS remain the same as approved in the SDFD Surveillance Use Policy.

## DEPLOYMENT LOCATION

During calendar year 2025, UAS flights occurred in all council districts.

## COMMUNITY COMPLAINTS OR CONCERNS

SDFD did not receive any complaints or inquiries regarding UAS operations in calendar year 2025.

## AUDITS OR INVESTIGATIONS

The UAS Program Manager conducted an annual audit for calendar year 2025 for all UAS operations. The results from the internal audit showed that authorized department personnel did comply with the Surveillance Use Policy. There were not any violations of the Surveillance Use Policy.

## DATA BREACH OR UNAUTHORIZED ACCESS

SDFD UAS and IT personnel did not detect any data breaches or unauthorized access to the data collected by the UAS.

## DATA BREACH DETECTION

The City's Department of Information Technology oversees the IT governance process and works with SDFD'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

SDFD was not notified of any data breaches relating to UAS data.

## PUBLIC RECORDS ACT REQUESTS

SDFD did receive one Public Record Act Requests in calendar year 2025 relating to UAS operations, PRA 25-3841. The request was made on May 19, 2025 and closed on June 18, 2025.

## ANNUAL COST

The SDFD UAS Program is staffed by full time personnel as a collateral duty and has not required the hiring of additional staff.

## REQUESTED MODIFICATIONS TO THE USE POLICY

SDFD is not requesting any modifications to the current UAS Surveillance Use Policy.

# Mission Bay and OB Pier UASI Camera System

**Department/Division: Fire-Rescue/Lifeguard Services**

**Subject Matter Expert: James Gartland, Lifeguard Chief**

**Phone Number and Extension: (619) 221 8832**

**Related Policy/Procedure:**

- Mission Bay and OB Pier UASI Camera System Surveillance Use Policy

## DESCRIPTION

The Mission Bay and Ocean Beach (OB) Pier Urban Area Security Initiative (UASI) Camera System (Camera System) has been purchased and installed. The purpose of this technology is for SDFD's Lifeguard Services Division to observe water-related emergencies and public safety concerns on both Mission Bay and in the Pacific Ocean, adjacent to the Ocean Beach Pier. The Camera System is intended to increase capabilities for public safety and emergency management. As of January 31, 2026, the Camera System installation is not complete, and the Camera System has yet to be operational. Pursuant to section 210.0108(c) of the San Diego Municipal Code, the Department is seeking continued approval for use the technology. The Department anticipates the OB Pier and Mission Bay Camera System to be activated and operational within the calendar year (2026).

## SHARING OF DATA

No sharing of data has occurred, as the Camera System is not yet operational.

## LOCATION

The Camera System was installed at the following locations:

OB Pier: 5100 Niagara Ave. San Diego CA 92107  GPS: 32.7502375 N, 117.2529870 W

Mission Point: 2600 Bayside Lane GPS: 32.76205 N, 117.24591 W

Quivira Basin: 2581 Quivira Ct. San Diego CA 92109 GPS: 32.76134° N, 117.24138° W

Dana Landing: 1800 Dana Landing Rd GPS: 32.76659 N, 117.23464 W

South Shores: 404 South Shores Parkway GPS: 32.76420 N, 117.21865 W

Fiesta Island: 3000 Fiesta Island Rd GPS: 32.76880 N, 117.20913 W

De Anza Cove: 3000 N. Mission Bay Dr. GPS: 32.79346 N, 117.20931 W

Ski Beach: 2900 Ingraham St. GPS: 32.77308 N, 117.23365 W

Vacation Island: 1404 Vacation Rd. GPS: 32.77193 N, 117.23981 W

Ingraham Street: Ingraham Street X Crown Point Dr. GPS: 32.77981 N, 117.23603 W

Santa Clara: 900 Santa Clara Pt. GPS: 32.78204 N, 117.24874 W

## UPDATES, UPGRADES, AND CONFIGURATION CHANGES

No updates, upgrades, or configurations have occurred, as the Camera System is not yet operational.

## DEPLOYMENT LOCATION

Installation is complete but the department has not activated the Camera System.

## COMMUNITY COMPLAINTS OR CONCERNS

SDFD did not receive any complaints or inquiries regarding the Camera System in calendar year 2025.

## AUDITS OR INVESTIGATIONS

No audits or investigations have occurred related to the Camera System, as the technology has yet to be operational.

## DATA BREACH OR UNAUTHORIZED ACCESS

SDFD did not detect any data breaches or unauthorized access to the data collected by the Camera System, as the Camera System is not yet operational.

## DATA BREACH DETECTION

The City's Department of Information Technology oversees the IT governance process and works with SDFD'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

SDFD was not notified of any data breaches relating to the Camera System, as the Camera System is not yet operational.

## PUBLIC RECORDS ACT REQUESTS

SDFD did not receive any Public Record Act Requests in calendar year 2025 relating to the Camera System.

## ANNUAL COST

During FY25, SDFD spent $239,135.63 in UASI Grant Funds to purchase the Camera System.

## REQUESTED MODIFICATIONS TO THE USE POLICY

SDFD requested the following modifications to the Camera System Surveillance Use Policy:

- Remove United States Customs and Border Patrol Agent and Naval Information Warfare Center Pacific Contractor from the list of authorized third-parties with access through the Joint Harbors Operational Center (JHOC);
- Clarify JHOC personnel's access to stored data. JHOC personnel do not have access to stored data, only a real-time video feed, unless required by law;
- Update the section on Third Party Data Sharing; and
- Articulate the role of San Diego Lifeguards as Public Officers, not Peace Officers, with very limited powers of arrest.