

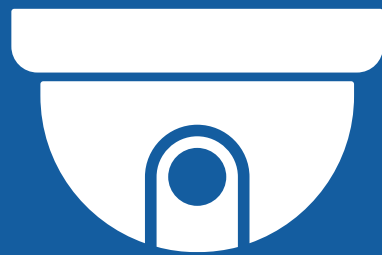


REVISED ANNUAL REPORT ON SDPD'S SMART STREETLIGHT & ALPR PROGRAM: IMPACT AND OVERSIGHT

Watch Commander's Office



WHAT IS SMART STREETLIGHT TECHNOLOGY?



SITUATIONAL AWARENESS CAMERAS

- Fixed view, no pan, tilt or zoom
- Records only public spaces, all other areas digitally masked
- No audio recording, gunshot detection, or facial recognition
- Data deleted after 13 days if not tied to an investigation



AUTOMATIC LICENSE PLATE READER (ALPR)

- Scans passing vehicles in public spaces
- Captures license plate and notable vehicle features
- Data is only accessed if related to an investigation
- Data deleted after 30 days if not tied to an investigation



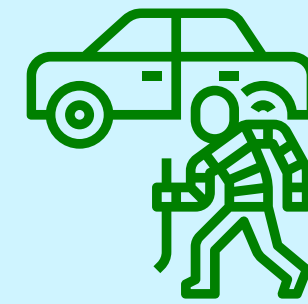
PROTECTING OUR COMMUNITY WITH TECHNOLOGY THAT WORKS



Has assisted in over **550 cases**, including homicides, robberies, burglaries, and attempted kidnappings.



Has aided in more than **390 arrests**, including 310+ suspected car thieves.

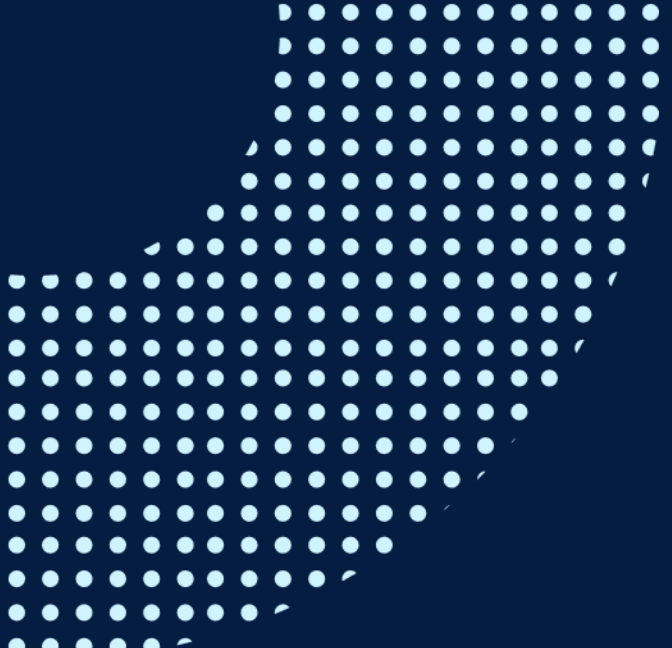


More than **410 stolen vehicles** recovered, and motor vehicle theft dropped **20 percent** last year.



BOOSTING EFFICIENCY AND EFFECTIVENESS

- **Minimizes Non-Essential Encounters:** Narrows search pools, helping avoid unnecessary public stops
- **Force Multiplier:** Enhances officer capability and investigative capacity
- **Cuts Costs:** Allows for precise searches, reducing the need for wide-area patrols and costly overtime
- **Supports Recruitment & Retention:** Officers want to work with investigative tools that boost their effectiveness and keep them safe



TRANSPARENCY AND SYSTEM ACCOUNTABILITY





PROGRAM LAUNCH AND EXISTING LEGAL FRAMEWORK

- The Smart Streetlights program was developed with several legal frameworks in mind:
 - **SB 54** – Prohibits police departments from being involved in immigration enforcement
 - **SB 34** – Sets strict rules for how ALPR data can be shared
 - **TRUST Ordinance** – Establishes local oversight and transparency requirements for surveillance technologies
- Camera installation began in December 2023
- All 500 cameras have been installed, and locations are publicly available online for full transparency

ANNUAL SURVEILLANCE REPORT AND DATA SHARING

- First Annual Report was submitted in February
- The Department openly disclosed ALPR data had been shared with federal and out-of-state agencies on a case-by-case basis for criminal investigations *not* related to immigration or reproductive care
 - Shared with CBP in cases involving kidnapping and human trafficking
 - Shared with HSI in cases involving drug trafficking and serious crimes against children
- After the report was published, the California DOJ contacted the department, and all such sharing has been halted

BRIEF ACCESS ERROR IDENTIFIED AND FIXED

- After submitting the Annual Surveillance Report, the Department discovered it had missed a brief period of unintended outside access caused by a Flock error at launch
- From Dec. 29, 2023, to Jan. 17, 2024, that error allowed CA law enforcement agencies to search SDPD's ALPR database
- No data was accessed or shared with federal or out-of-state agencies during this period.
- The issue was discovered through an internal audit, and the setting was immediately fixed
- Once the omission was identified, the Department notified the Privacy Advisory Board and resubmitted the report
- Has not occurred since



STRENGTHENING AUDITS, POLICY & COLLABORATION



Actions taken

- Stopped all sharing with federal and out-of-state agencies for all cases
- Issued department-wide directive reiterating that stance in May
- Issued department-wide order on TRUST Ordinance auditing requirements in April



Actions in progress

- Amended the ALPR Use Policy to clarify sharing restrictions
- Commitment to exploring ways to improve the auditing process
- Currently working with the Privacy Advisory Board to ensure transparency, detailed annual reporting and that data remains secure.

ALPR DATA SECURITY



DATA ACCESS

- Only accessed during an investigation
- Only accessed by trained, authorized users
- Weekly audits by a system administrator
- Rotating single sign-on (SSO) password-protection
- Minimum password requirements



SECURITY COMPLIANCE

- AWS Government Cloud
- SOC 2 Type II
- ISO 27001:2022
- NIST 800-53
- NIST 800-53 Rev 5
- HIPAA
- VPAT
- CISA: Secure-by-Design Pledge
- CJIS CSP Compliant





AUDIT PROCESS



Audit Overview

- Conducted by a Supervisor (Sergeant)
- Done weekly
- Checks for user compliance with state and local laws, including compliance with the Use Policy
- Ensures equipment is functioning properly
- Data is not being retained beyond 30 days
- The system is only accessed by authorized users



Case and Event Numbers

- Verify case or event number
 - Check to see if it is current
 - Repeat use of a case or event number
 - Verify reason for search with outside agency case numbers

KEY TAKEAWAYS

- This industry-standard technology is a proven crime-fighting tool, locally and nationally
- SDPD has updated its ALPR Use Policy and is committed to strengthening its auditing processes in collaboration with the PAB
- The Department has not and will not use this technology to assist the federal government with any kind of immigration or reproductive care investigation
- SDPD recognizes and respects the role of our oversight board and City Council in this process



QUESTIONS?

