Privacy Advisory Board

MEMORANDUM

November 5, 2025

To: The Hon. Council President LaCava and Members of the San Diego City Council

From: City of San Diego Privacy Advisory Board

RE: PAB Review and Recommendation of the San Diego Police Department's **Amended 2025 ALPR Annual Surveillance Report**

I. Recommendation

The Privacy Advisory Board (PAB) recommends that the City Council cease the use of Automated License Plate Recognition technology ("ALPR") until completion of the modifications to the amended 2025 ALPR Annual Surveillance Report summarized in section II and detailed in section III, below.

The PAB highlights to the City Council that Flock, as the ALPR vendor and SDPD as the user are not in compliance with the TRUST Ordinance. PAB also urges further revisions to the ALPR Annual Surveillance Report to increase transparency, provide more fulsome compliance with the TRUST Ordinance's requirements for the Annual Surveillance Reports, increase the usefulness of the Annual Surveillance Report to the public, policy makers, and the media, and provide other City departments with an example of best practices in completing Annual Surveillance Reports. These further revisions are detailed in section IV, below.

II. Overview and General Comments

The SDPD has worked closely with the PAB to improve the content of the ALPR Annual Surveillance Report in accordance with the PAB's recommendations and the TRUST Ordinance. The PAB appreciates this cooperation. The PAB also has received considerable input from the public that has proven invaluable in fully understanding the impact ALPRs can have on San Diego's many communities. The PAB urges continued cooperation with the SDPD and the public to further refine and analyze the use of Surveillance Technologies in the City.

To continue use of ALPRs, the following actions must be taken to comply with the TRUST Ordinance and the ALPR Use Policy:

1. Obtain a written attestation from the vendor, Flock Safety, that it:
   a) currently.is.and.has.complied.with.the.ALPR.Use.Policy¡.
   b) has.not.shared.any.SDPD.ALPR.data.with.any.third.party.and.no. third. party. has. accessed. SDPD. ALPR. data? other. than. that. already.reported.in.the.ALPR.Annual.Surveillance.Report¡
   c) There. have. been. no. data. breaches. or. other. unauthorized. access.of.the.data¡.
2. Periodically conduct routine third-party risk management and oversight of the ALPR services Flock Safety provides. This includes review of audit reports generated by Flock Safety, such as SOC 2 Type 2 audit reports.
3. Provide a comprehensive summary of community complaints and concerns and a response to those complaints and concerns. The Annual Surveillance Report does not comprehensively summarize these criticisms or sufficiently respond to them. Responses may include explaining why the concerns have been addressed in the Use Policy or explaining why the SDPD believes that despite the concerns, the benefits of ALPR's outweigh the risks expressed. Addressing these concerns goes to the heart of the TRUST Ordinance.
4. Develop clear written protocols detailing responsibilities between the SDPD and the City's Department of Information Technology ("City IT Department"). The SDPD is responsible for all IT controls. While it may be reasonable in exercising that responsibility to delegate tasks to qualified third parties, the responsibility itself remains with the SDPD. Therefore, if not already in existence, the SDPD should develop written policies and procedures delineating tasks and responsibilities between the SDPD and the City IT Department.

Beyond these issues, the other recommendations listed in section IV are intended to increase transparency, accountability, and compliance with the TRUST Ordinance through improvements in the Annual Surveillance Report. An Annual Surveillance Report should be the one resource that the public, the media, the City Council, other policy makers, members of PAB, and other City departments and agencies consult to fully understand a given Surveillance Technology, its use, its risks, and its benefits.

The ALPR Annual Surveillance Report should be a model report for all others to follow, especially given the privacy, civil rights, and civil liberty violations that can result from the misuse of ALPR data and the history of the public's concerns surrounding this surveillance technology.

Finally, Municipal Code §210.0108(b) requires the PAB to consider annually the following: (1) whether the benefits to the community of each item of approved surveillance technology outweigh the costs; (2) whether civil rights and civil liberties are being safeguarded; and (3) whether use of the surveillance technology, in accordance with the approved Surveillance Use Policy, should continue, cease, or be modified to address identified concerns. Of these, the risk-benefit analysis for ALPRs are the most challenging because of a lack of historical data and the complexity of performing this type of analysis as applied to crime and crime-fighting trends. The PAB urges the SDPD to continue to develop measures of the benefits and limitations of this technology, its deployment, and meaningful quantifications of its costs and benefits, including key performance indicators.

Timeframe: We urge the City Council to act immediately to have the SDPD address the issues noted above and below.

III. Significant Concerns to be Addressed

Attestation Letter from Flock Safety. Flock Safety is the vendor responsible for collecting, analyzing, and storing data, maintaining the ALPR system, and developing and maintaining the user interface. Flock Safety also is contractually obligated to comply with the ALPR Use Policy. The SDPD indicates in the Revised Annual Surveillance Report that "Flock Safety adheres to all applicable cybersecurity industry standards, attestations, and frameworks" and meets the City IT governance requirements based on the 2023 procurement process. To increase accountability, ensure adequate vendor oversight, and fulfill its reporting requirements under the TRUST Ordinance, the SDPD must obtain written attestation from Flock Safety that Flock has fulfilled its obligations regarding ALPR data maintenance and safety. Specifically, Flock Safety should attest that it:

a) currently is and has complied with the ALPR Use Policy, as contractually required.

b) has not shared any SDPD ALPR data with any third party and that no third party has accessed SDPD ALPR data, other than already reported in the ALPR Annual Surveillance Report.

c) There have been no data breaches or other unauthorized access of the data.

This attestation should be provided at least annually. There is no practical independent way to confirm whether anyone other than Flock Safety and its authorized users can or has accessed the ALPR data stored on Amazon Web Services (AWS). Although Flock's documentation refers to audit logs, these logs likely exist only within each customer's own isolated AWS environment ("tenant-specific instance"). This means the logs show access activity inside the SDPD's portion of the larger Flock system housed on AWS servers, but not at the broader AWS platform level. This is a reality of third-party web-based servers. Requiring attestations is a common and commercially reasonable means of addressing this issue.

Routinely Conduct Vendor Risk Management Review and Oversight. The SDPD should designate a qualified person to conduct third-party risk management reviews and oversight of the ALPR services provided by Flock Safety. Internally, Flock Safety conducts various audits, such as SOC 2 Type 2 audits. However, it does not appear that anyone within the City is reviewing these audits. Given the sensitive nature of the information at issue, the audits should be reviewed by a person with sufficient education and training in cybersecurity. Here, for example, the SOC 2 Type 2 audit report Flock Safety provided did not address the "Privacy" Trust Services Criteria in the audit report (or, by extension, "Processing Integrity," which is also not part of the report). Given that ALPRs raise significant privacy concerns, the omission of that specific Trust Services Criteria is significant and should be addressed.

If the SDPD does not employ such a person, the City's Department of Information Technology ("City IT Department") may have such a person and should be designated. If no qualified person exists, one should be retained.

Attached as Exhibit A is an example of a tool that can be used by the designated qualified person to conduct a review.

Comprehensive Summary of Community Concerns and Complaints with a Response. Communities throughout San Diego have expressed alarm over the use of surveillance technologies. These concerns have become far more pronounced and widespread given the federal government's aggressive and unprecedented policies and tactics targeting U.S. citizens, documented and undocumented immigrants, people of color, and communities that historically have been overpoliced. Moreover, San Diego's vendor, Flock Safety, has faced significant criticism. Some cities have refused to deploy ALPR systems or refused to contract with Flock Safety, while others have cancelled or not renewed contracts with Flock Safety. In expressing their concerns and complaints, San Diego residents have included the experiences of other cities as examples to follow. However, the Annual Surveillance Report does not adequately describe and summarize the concerns and complaints raised and has not directly addressed them.

The TRUST Ordinance requires that these concerns and complaints be addressed. See SDMC §210.0102(a)(6). The PAB believes that doing so will help increase trust between the SDPD and impacted communities. A proper response might include explaining why a concern or complaint does not apply under the ALPR Use Policy or if it does, how, in the view of the SDPD, the benefits of the ALPR system outweigh the concern or complaint.

Clear Delineation of Responsibilities Between the SDPD and the City IT Department. The SDPD generally references the City's IT governance process (found in the FY23–FY27 IT Strategic Plan) and indicates that it works closely with the City's IT Department "to assess cybersecurity risks, approve technology, and ensure proper governance." While the PAB does not question this, it is not aware of a written delineation of the duties and responsibilities between the departments. The responsibility for protection and proper use of ALPR data resides with the SDPD and it cannot delegate that responsibility to another party. It can, however, delegate to appropriate parties the tasks that must be performed for it to fulfill its responsibility. A lack of a clear written delineation of duties and responsibilities between the departments can result in oversights and mistakes. Organizations frequently have written policies and procedures that specify the duties and responsibilities of an IT department and the other entity to minimize the risk of error. If one does not currently exist, one should be created. If one does exist, it should be submitted to the PAB for review.

IV. Recommended Modifications to the Annual Surveillance Report

The PAB recognizes the considerable effort taken in compiling the latest version of the Annual Surveillance Report. The task is time-consuming and made more difficult because the City lacks a paid professional privacy staff, leaving the task of TRUST Ordinance compliance to personnel who may not have the requisite specialized education, training, and expertise.

To improve the Annual Surveillance Report and create a "best practices" model to be used by other City departments in reporting on their surveillance technologies, the PAB request that the following be done:

- Enter into a new, separate contract with Flock Safety (or any vendor providing ALPR services) that more fully sets forth the duties and responsibilities of the contracting parties, including the vendor's audit and reporting requirements owed to the City and the SDPD. The current contract with Flock Safety is merely an addendum to a contract with the vendor providing Smart Streetlights, Ubicquia, and does not reflect contracting best practices.
- Number the headings to match the numbered requirements of section 210.0102(a) of the TRUST Ordinance

- Continue to include a clear and simple heading that summarizes the prompt of the TRUST Ordinance requirements. However, add the full text of each category listed in SDMC 210.0102(a). This can be done as part of the headings or in footnotes.
- Organize the categories of responses in the same order set forth in SDMC 210.0102(a). This makes finding information much easier.
- The description of the technology section should be simpler and clearer. It should be a straightforward explanation of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology. It should explain what the technology does, and all the information gathered and processed. It should not contain a summary of the overall report and should not contain any advocacy in favor of using the technology. If the SDPD wishes to include this other material, it should do so elsewhere in a clearly delineated section of the report.
- Include a section for each category listed in SDMC 210.0102(a), even if it repeats information contained elsewhere. This also makes finding information much easier.
- In "Sharing Data" and Addendum A, pursuant to SDMC §210.0102(a)(2), for each occasion data was shared, include the type of data disclosed, under what legal standards the information was disclosed, and the justification for the disclosure.
- At page 10 concerning the information and statistics section, contextualize the data provided against standard crime statistics. For example, the ALPR's assisted with 11 homicides, but how many homicides are there annually?
- At page 10, is there any historic data about opening and closing cases that can be used to indicate the effectiveness of ALPRs? Even imperfect data may be useful in evaluating ALPR effectiveness, which is a key indicator of the benefits of the technology.
- Ensure the SDPD has sufficient technical capabilities to comply with the TRUST Ordinance for all surveillance technologies operated by the SDPD. A lack of privacy expertise within the City presents a significant challenge to the oversight and use of Surveillance Technologies and the data they collect. Other cities address this challenge through retention of a professional staff of privacy experts.

Exhibit A

Statement of Standards for Attestation Engagements (SSAE) 18
&
System and Organization Controls (SOC) 2
Audit Report Review Form

1. PURPOSE

The purpose of this SSAE 18 SOC 1 and/or SOC 2 Service Provider Audit Review Form is to assist [insert name] management (the 'Company') with its evaluation of the internal controls over financial reporting and other governance objectives that relate to the use of material service providers and the service provider's sub-service providers (if/where applicable).

The Statement of Standards for Attestation Engagements (SSAE), as updated from time to time by the American Institute of Certified Public Accountants (AICPA), outlines attestation standards for these reviews. The service provider may have a System and Organization Control (SOC) report based on the SSAE standard. SOC audits may be noted as Type 1 (the design of the control environment) or Type 2 (the design and operating effectiveness of the control environment). SOC 1 audits report on internal controls over financial reporting (ICFR), and SOC 2 audits report on Trust Services Criteria (TSC), specifically Security, Availability, Processing Integrity, Confidentiality, and Privacy. Where the service provider does not have an audit report, alternate assessment procedures may be performed.

2. GENERAL INFORMATION

Name of Service Organization:	
Name of Service Auditor Organization:	
Description of the services provided by the service organization and/or the types of transactions processed by the service organization:	
Identify the significant financial statement accounts, business processes, and/or IT-related systems and the disclosures and relevant assertions affected by transactions processed by or services delivered from the service organization.	
Sub-service providers identified in the audit report and the audit status (e.g., included in the audit report or not audited):	
Report type or description of alternative review procedures if no audit report is available:	☐ SSAE 18 SOC 1 Type 1 ☐ SSAE 18 SOC 1 Type 2 ☐ SOC 2 Type 1 ☐ SOC 2 Type 2 ☐ Alternate Procedures Required
Control objectives referenced in the audit report (please indicate the specific pages where the controls are documented):	
Trust Services Criteria addressed:	☐ Availability ☐ Security ☐ Processing Integrity

	☐ Confidentiality ☐ Privacy
"As of" date for the description of service organization controls:	
The date range for which the description of controls applies (this should be consistent with the audit period of [insert name]).	
Opinion type:	☐ Unqualified ☐ Qualified ☐ Adverse
Period covered by the service auditor's tests of control operating effectiveness:	
Indicate the nature of the opinions rendered and whether these included any modifications to the standard reporting language.	

3. PROCEDURES

Read the service auditor's audit report and assess its implications for the Company's assessment of internal control effectiveness, and indicate whether compliance was found for the following:	Complies	
	Yes	**No**
Indicate whether the service auditor prepared a Type 2 report.	☐	☐
Indicate whether the description of services includes coverage of the following COSO principles:	☐	☐
• Control Environment	☐	☐
• Risk Assessment	☐	☐
• Control Procedures	☐	☐
• Monitoring	☐	☐
• Information and Communication	☐	☐
Indicate whether the description of services is sufficiently detailed to understand how the service organization's processing affects the Company's internal control over financial reporting.	☐	☐
Indicate whether the description of controls is adequate to provide an understanding of those elements of the Company's accounting information system or other services maintained or impacted by the service organization.	☐	☐
Identify control testing exceptions and determine whether they indicate a control deficiency.	☐	☐

4. COMPLEMENTARY USER ENTITY CONTROLS (CUECs)

If the description lists complementary user entity controls (CUECs), which must be in place for the user entity to obtain reasonable assurance that the service organization's controls are valid, summarize those CUECs in the table below. Indicate the pages where the CUECs are described in the audit report. Assess the design and operating effectiveness of the identified CUECs for the reporting period. Add each CUEC identified in the service auditor's report below. Add rows for additional CUECs. Where a CUEC is not applicable to the operating environment, provide a brief description of the rationale.

CUECs and Status at [insert Name]	Design	Operation	N/A
CUEC 1	☐	☐	☐
CUEC 2	☐	☐	☐
CUEC 3	☐	☐	☐
CUEC 4	☐	☐	☐
CUEC 5	☐	☐	☐

5. REVIEW OF THE SERVICE AUDITOR'S REPORT

The following summarizes the opinions provided in the service auditor's report.

Required Opinion	Service Auditor Opinion	
	Standard	**Modified**
Indicate whether the service organization's description of its controls presents fairly, in all material respects, the relevant aspects of the service organization's controls that had been placed in operation as of a specific date.	☐	☐
Indicate whether the controls were suitably designed to achieve specified control objectives.	☐	☐
Indicate whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the testing period specified.	☐	☐

Describe any modifications to the service auditor's standard opinion and the effect these modifications have on the Company's assessment of internal control effectiveness.

Table 1 - Modifications to the Service Auditor's Report (if applicable)

6. REVIEW OF THE SERVICE ORGANIZATION'S DESCRIPTION OF CONTROLS

	Internal Control Component							
	Control Environment		Risk Assessment		Information and Communication		Monitoring	
	Yes	No	Yes	No	Yes	No	Yes	No
Transactions, processes, computer applications, or business units that affect the Company's assessment of internal control effectiveness are described in the audit report.	☐	☐	☐	☐	☐	☐	☐	☐
The level of detail provided is sufficient to allow the Company to understand how the service organization's processing affects the Company's internal control.	☐	☐	☐	☐	☐	☐	☐	☐
The audit report identified no changes to controls since the later date of the last service auditor's report or within the last 12 months.	☐	☐	☐	☐	☐	☐	☐	☐
The audit report identified no instances of noncompliance with the service organization's controls identified in the service organization's description of controls.	☐	☐	☐	☐	☐	☐	☐	☐

7. RECOMMENDATIONS RELATED TO THE COMPANY'S USE OF THE SERVICE PROVIDER

Use the table below to indicate any recommendations or risks identified with the use of the service provider's services.

Table 2 - Recommendations

8. REVIEW & APPROVAL

Management Review and Approval By:			
Name	**Signature**	**Title**	**Date**

9. REVIEW & ACKNOWLEDGEMENT

This form summarizes the procedures performed and the conclusions reached on the effectiveness of internal controls and/or Trust Services Criteria maintained at the service organization, as documented in a service auditor's [insert audit report name] report.

Employee Name:

_____

Employee Title:

_____

Employee Signature:

_____

Date:

_____