THE CITY OF SAN DIEGO

M E M O R A N D U M

DATE: February 20, 2025

TO: Ike Anyanetu, Chair, Privacy Advisory Board

FROM: Eric Portnoy, Lieutenant, Research Analysis, and Planning

SUBJECT: The San Diego Police Department's Response to the Privacy Advisory Board's questions titled "*Questions by PAB Member Brett Diehl re: SDFD & SDPD Annual Surveillance Reports*."

Summary:

The Transparent and Responsible Use of Surveillance Technology (TRUST) Ordinance mandates, "City staff shall submit to the Board and to the City Council by February 1 of each year an Annual Surveillance Report that discusses the new surveillance technology and existing surveillance technology approved on or after January 1 of the prior year and that provides additional, necessary updates to the surveillance technology approved in prior years."

On February 1, 2025, the San Diego Police Department (SDPD) submitted the 2024 Annual Surveillance Report to the City Council President, Councilmembers, Chair of the Privacy Advisory Board (PAB), and PAB members, in compliance with the Ordinance. Following the submission of the Annual Surveillance Report, PAB provided numerous written questions to the Department titled "*Questions by PAB Member Brett Diehl re: SDFD & SDPD Annual Surveillance Reports*."

This memorandum will outline each PAB question, followed by SDPD's response.

1. **<u>Unmanned Aerial Systems (UAS):</u>**

"At the other 37 incidents the UAS camera technology was used for observation only and did not record any evidence." (p. 13):

A. **When, by whom, and according to what criteria is the decision made regarding if to record evidence?**

As stated in each of the 16 individual UAS Use Policies' under "Data Collection" section, *"UAS are deployed only to specific incidents with a specific target or specific objective. The UAS Pilot manually controls the UAS camera system and activates either video or photos to be captured based on the objectives and goals of the UAS mission. During a UAS Evidence Collection Operation, the UAS Pilot will manually control the UAS to take photographs or video as requested by the investigative unit that requested UAS Support.*

During a law enforcement operation or during observation of a crime or in anticipation of a crime, the UAS Pilot will manually activate the video recording capability of the UAS in a similar manner to how a ground-based officer activates their Body Worn Camera during a contact. This captured video is regarded as Digital Media Evidence (DME) and is treated as evidence throughout the remainder of the operation until the DME is properly impounded and documented by the UAS staff assigned to the operation.

During observation and overwatch support of High-Risk Tactical Operations, the UAS Pilot will manually control the UAS to take a video of the entire operation to record all police activity during the incident. During UAS safety and enhanced security overwatch operations at special events and other large gatherings, the UAS Pilot generally does not activate video recording unless necessary to record a law enforcement contact, a crime occurring or in anticipation of a crime.

During all operations, the UAS Pilot is trained to make every effort to only capture visual imagery of the law enforcement contact or intended target of observation in order to protect the privacy of nearby uninvolved citizens and their property."

B. **Is this decision made before the UAS is deployed?**

See the response to Question 1.A. above.

2. **<u>Covert Audio Recording Devices (p. 20):</u>**

A. **What percentage of the 128,814 collections were authorized by a court-issued order (warrant, wiretap order, etc.)?**

The Covert Audio Recording Devices (Record Only) were only utilized twice during the 2024 calendar year. <u>The information below was mistakenly put in the wrong section:</u>

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.

This information was for the Covert Cloud Based Mobile Application (CBMA) information.

As stated in the Covert Cloud-Based Mobile Application Use Policy under "Use" (p.1), "*The CBMA can be used for audio recordings of law enforcement personnel, undercover operators, victims, and witnesses who engage with persons suspected of engaging in criminal activity. This also includes real-time audio monitoring and GPS location by law enforcement officers, which provides additional security and safety to undercover operators.*

CBMA shall only be used for official law enforcement business. No personal use is authorized.

The CBMA can be used for audiovisual recordings of law enforcement personnel, undercover operators, victims, and witnesses who engage with persons suspected of engaging in criminal activity. This also includes real-time audiovisual monitoring by

law enforcement officials, which provides additional security and safety to the undercover operators."

The Covert Cloud Based Mobile Application (CBMA) 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. The Department utilized 107 lines in the 2024 calendar year.

During the utilization of the 107 lines, 128,814 calls and texts were recorded/captured during the 2024 calendar year.

The two main uses for this technology are to record and document undercover police operations and controlled calls during criminal investigations. Regarding undercover operations, the recording would be of police activity in a place the detective had a lawful right to be. Therefore, no warrant is required.

Regarding controlled calls (recording of a conversation between a victim and suspect), California Penal Code Section 633 allows for government agents to record such calls when acting in the course and scope of their employment and lawfully recording any communication that they could lawfully overhear or record. Therefore, no warrant would be required, and the evidence would be admissible in court.

B. **If there are instances where these devices are used without court oversight, what criteria does SDPD use to determine how to appropriate deploy this technology, and who is the determining authority on such decisions?**

See the response to Question 2.A. above.

3. **PTZ Cloud Based System (p. 20), Trail cameras (p. 20), and Covert Audio/Visual Recording Devices (p. 21):**

A. **What and how many of these devices does SDPD maintain?**

The Department will not be releasing these figures due to operational security as they covert technologies.

B. **Because the technologies are not being utilized, is there a plan for SDPD to stop possessing such equipment?**

These systems were not utilized in the calendar year 2024, however, they have specific uses and can be utilized in the future. There is no plan in place to stop possessing this technology.

4. **CP Clear and TLOxp (p. 41):**

A. **Does each user have their own login credentials?**

Yes, each authorized user of both TLOxp and CP Clear are required to have unique login credentials, used each time upon accessing the systems.

B. **Do these technologies keep/create a log of which users access what information?**

Yes, both technologies maintain a log of all user activity within the application, to include search parameters and justifications.

C. **Is such information audited to ensure searches are not being run for inappropriate reasons (such as retaliation, harassment, personal vendetta, etc.)?**

As stated in the Auditing and Oversight section of the Use Policies for CP Clear and TLOxp, "*An audit can be performed by site administrators on an as-needed basis. Users who leave the department have their access removed. At the point of conducting an inquiry, a field titled "Reference" serves as a method to demonstrate the user's "need to know, right to know" by providing case numbers, incident numbers, or other unique identifiers."*

Both technologies will be regularly audited for appropriate usage as overseen by the Research, Analysis, and Planning unit.

5. **Automated License Plate Recognition (p. 48/57):**

A. **Are the data records stored on Vigilant's servers or locally on SDPD servers?**

As stated in the Vigilant Surveillance Use Policy under "Use" (p.1),

"The San Diego Police Department only has access to the data Vigilant obtains from other agencies/companies that share their data with Vigilant. The Department does not collect, capture, or record any data. It is an analytic tool to help investigators review data returns from a variety of ALPRs in the State of California to enhance their investigations.

The San Diego Police Department does not own any of the data nor does it provide any data to Vigilant."

The Surveillance Use Policy states, under "Data Collection" (p. 1 & 2),

"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."

Regarding data retained for investigative or enforcement functions, this is covered in the Vigilant Surveillance Use Policy under "Data Retention" (p.2), which states,

"San Diego Police Department personnel working in an investigative or enforcement function often retain data relevant to an investigation acquired through Vigilant.

Any data retained shall follow Department Procedure 4.13 – Retention / Custody of Officer Notes, Documents, and Other Evidence."

B. **Does Vigilant reserve any rights to make use of the data collected?**

As stated in the Vigilant Surveillance Use Policy under "Use" (p.1),

"The San Diego Police Department only has access to the data Vigilant obtains from other agencies/companies that share their data with Vigilant. The Department does

not collect, capture, or record any data. It is an analytic tool to help investigators review data returns from a variety of ALPRs in the State of California to enhance their investigations.

The San Diego Police Department does not own any of the data nor does it provide any data to Vigilant."

C. **Over 140,000 searches were done of ALPR records:**

(1) **Are there criteria for what types of investigations can make use of ALPR records?**

As stated in the Automated License Plate Recognition (ALPR) Surveillance Use Policy under "Use" (p. 1),

"ALPR systems have proven to be very effective tools in combating crime. The operation and access to ALPR data shall be for official law enforcement purposes only. The legitimate law enforcement purposes of ALPR systems include:

• Locating stolen vehicles, wanted vehicles, or vehicles subject to investigation and,

• Locating vehicles belonging to suspects, witnesses, and victims of a violent crime.

The San Diego Police Department will also use ALPR systems to enhance and coordinate responses to active critical incidents and public threats (e.g., active shooter, terrorist incident), safeguard the lives of community members by using this technology to locate at-risk missing persons (including responding to Amber, Silver, and Feather Alerts) and to protect assets and resources of the City of San Diego."

(2) **What is the standard of suspicion required to search an individual vehicle's ALPR history?**

As stated in the Automated License Plate Recognition (ALPR) Surveillance Use Policy under "Use" (p. 1),

"ALPR systems have proven to be very effective tools in combating crime. The operation and access to ALPR data shall be for official law enforcement purposes only. The legitimate law enforcement purposes of ALPR systems include:

• Locating stolen vehicles, wanted vehicles, or vehicles subject to investigation and,

• Locating vehicles belonging to suspects, witnesses, and victims of a violent crime.

The San Diego Police Department will also use ALPR systems to enhance and coordinate responses to active critical incidents and public threats (e.g., active shooter, terrorist incident), safeguard the lives of community members by using this technology to locate at-risk missing persons (including responding to Amber, Silver, and Feather Alerts) and to protect assets and resources of the City of San Diego."

(3) **What limitations are placed on investigators ability to query ALPR history?**

As stated in the Automated License Plate Recognition (ALPR) Surveillance Use Policy under "Use" (p. 1 & 2),

"The following uses of ALPRs shall be expressly prohibited:

• To invade the privacy of individuals or observe areas where a reasonable expectation of privacy exists.

• To be used in a discriminatory manner and to target protected individual characteristics, including race, color, ethnicity, religion, national origin, age, disability, gender (to include gender identity and gender expression), lifestyle, sexual orientation, or similar personal characteristics, in accordance with Department Policy 9.33.

• To harass, intimidate, or discriminate against any individual or group.

• To violate any Constitutional rights, federal, state, or local laws (e.g., California Values Act, FACE Act, etc.)

• To be utilized for any personal purpose.

• To investigate parking violations and conduct traffic enforcement.

• To indiscriminately view video without investigative or administrative need."

6. **Body Worn Camera (p. 64):**

A. **The cost of the BWC is anticipated to nearly double (from $1.1 million to $2.2 million from FY24 to FY25):**

The previous contract with Axon ended at the end of fiscal year 2023. The $1.1 million was an extension for the end of that contract, from July 1, 2023, to January 2024. This was not for a full fiscal year, as it was only an extension.

The $2.2 million cost is due in 2025 for a full year.

B. **What changes in procurement or use underlie this increase?**

No changes were made to procurement or use. Please see the response above for further details on the cost increase.

C. **Are software changes part of this cost increase?**

Software changes are not part of the increase.

7. **Vehicle and Object Trackers (p. 88):**

A. **In how many of the cases during FY24 did SDPD seek a warrant before attaching a tracker to a vehicle or other object?**

The SDPD did not capture the data regarding how many tracker warrants were sought during the 2024 calendar year.

B. **For individuals subject to a Fourth Amendment waiver, what are the criteria used in evaluating if placement of a tracker is appropriate?**

The Object Trackers can only be used after a tracker warrant has been acquired, the subject's 4th Waiver status is verified, or consent is obtained.

The Vehicle Trackers can only be used after a tracker warrant has been acquired or the subject's 4th Waiver status is verified.

If the 4th Amendment Waiver status is utilized for tracker placement, the case agent must articulate that the vehicle or object is solely utilized by the subject with the 4th Amendment Waiver. If during an investigation, a vehicle tracker is placed on a vehicle solely driven by the subject with a 4th Amendment Waiver and it is later determined the vehicle is occasionally driven by another person without a 4th Amendment Waiver, a tracker warrant must be sought and approved to continue utilization of this technology.

Trackers are frequently checked out from the Robbery Unit for large scale operations. Detectives can utilize them multiple times during a single operation, and a tracker warrant can be sought and approved for multiple subjects.

As stated in the Object Tracker Surveillance Use Policy (p. 1),

"Object Trackers are issued to San Diego Police Department (SDPD) members for a limited duration during the course of a specific criminal investigation. Object Trackers are used to locate stolen property and to locate suspects who possess the stolen property. The trackers can be monitored by an authorized user and/or Communications can be alerted to assist personnel to track the device once the device is activated and begins to move.

When a tracker is requested by a SDPD member, a Special Equipment Technician of the Robbery Unit is assigned the request. The technician speaks with the SDPD Member to fully understand the mission of how the device will be used. The request is evaluated for equipment suitability and legal standing. If equipment deployment is appropriate, a request form is completed stating the crime being investigated and the legal authority to use the Object Tracker. The request form also states all personnel authorized to monitor the equipment.

All requests for an Object Tracker must be approved by a Robbery Unit sergeant and a Robbery Unit lieutenant. The program administrator will grant authorization to all required members to monitor the device and create the required reports about possible evidence collected from the device."

As stated in the Vehicle Tracker Surveillance Use Policy (p. 1)

Vehicle Trackers are used to track vehicles involved in a criminal investigation by placing a tracker on the vehicle and obtaining GPS location data from the device. The trackers currently in use are provided by 3SI. Vehicle Trackers are generally issued to an SDPD member for a limited duration during the course of a specific criminal investigation. However, these devices may be issued to a specific unit on a permanent

basis to facilitate logistical issues associated with needs arising during off-hour and short-notice deployments.

When a tracker is requested by an SDPD member, a Special Equipment Technician of the Robbery Unit is assigned the request. The technician will speak with the SDPD member to fully understand the mission of how the device will be used. The request is evaluated for equipment suitability and legal standing. If equipment deployment is appropriate, a request form is completed stating the crime being investigated and the legal authority to use the tracker. It is important to note that vehicle trackers can only be deployed with a warrant or if the subject of the tracking device is a Fourth Amendment waiver. The request form will also state all personnel are authorized to monitor the equipment.

All requests for a Vehicle Tracker must be approved by a Robbery Unit sergeant and a Robbery Unit lieutenant. The program administrator will grant authorization to all required members to monitor the device and create the required reports about the evidence collected.

Conclusion:

The SDPD has carefully considered and responded to these questions put forth by PAB and looks forward to presenting this Annual Report in front of the City Council.

Please contact Lieutenant Portnoy if additional questions arise.