SAN DIEGO POLICE DEPARTMENT
ORDER

DATE/TIME: APRIL 25, 2025 1000 HOURS

NUMBER: OR 25-13

SUBJECT: AUDITS & INSPECTIONS OF SURVEILLANCE TECHNOLOGIES

SCOPE: ALL MEMBERS OF THE DEPARTMENT

DEPARTMENT PROCEDURE AFFECTED: SDPD INSPECTION MANUAL

Portions of this document are deemed by the San Diego Police Department to be exempt from public disclosure because the public interest served by not disclosing the information clearly outweighs the public interest served by disclosure, pursuant to California Government Code section 7922.000.

To better govern the responsible utilization of the San Diego Police Department's approved technologies which fall under the City of San Diego's Transparent and Responsible Use of Surveillance Technology (TRUST) Ordinance, the units that manage the specific surveillance technology will audit/inspect them on at least a quarterly basis.

To prepare for the required Annual Report each year, as set forth in SDMC 210.0108, the managing unit (The managing unit is the person(s) recognized as the Subject Matter Expert (SME) for the TRUST Ordinance reporting or who controls the equipment) shall continually track and document the following types of information, as listed in SDMC 210.0102:

1. **Quantity of data:** A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the surveillance technology.

2. **Name of the Recipient of Data, Legal Standards, etc.:** Whether and how often data acquired through the use of the surveillance technology was shared with any non-City entities (e.g. District Attorney or other Law Enforcement Agencies), the name of any recipient entity, the types of data disclosed (e.g. Body Worn Camera footage, drone footage, data reports, etc.), under what legal standards the information was disclosed (e.g. warrant, criminal discovery process, etc.), 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. **Physical Deployment:** 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. **Software updates, hardware upgrades, reasoning for the change:** 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.

4. **Where the tech was deployed geographically:** A description of where the surveillance technology was deployed geographically, by each City Council District or police area, in the applicable year.

5. **Community Complaints or Concerns:** 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.

5. **Data breaches or Improper Use:** 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.

6. **Crime Statistics:** Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes. (This includes any success stories of the use of the technology.)

7. **CPRAs:** 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.

8. **Cost:** 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.

Effective immediately, the managing unit will conduct, at least, quarterly audits/inspections, which will include:

1. Selecting a minimum of 10 different uses of the technology, if applicable, within the timeframe, to confirm that protocols are being followed by department members who have access to surveillance equipment or software, following the criteria set forth in the technology's approved Use Policy.

    a. If the surveillance technology was used less than 10 times in the audit period, all uses shall be audited.

2. All managing units shall maintain, to the extent possible, a log of what data is shared with non-City entities as referenced in the Transparent and Responsible Use of Surveillance Technology (TRUST) Ordinance. San Diego Municipal Code § 210.0102(a)(2) and (c). For example, the District Attorney's Office or other Law Enforcement Agencies are considered non-City entities under the TRUST Ordinance. City entities include any Department or staff member within the City of San Diego, including the City Attorney's Office, San Diego Fire-Rescue, etc.

3. All managing units will also review their approved Use Policy and confirm adherence to the policy. If any activity is outside of the scope of the Use Policy, it shall be immediately addressed and annotated for potential modification of the Use Policy during the Annual Report.

Audit/Inspection Documentation:

At the beginning of the quarter (April, July, September, and January) the Research, Analysis, and Planning (RAP) Unit will send out an email to all identified SMEs/Managing Units. The email will contain an audit form to be completed by the SME/Managing Unit.

1. These audits shall be submitted by the 15th of the month following the audit period (April 15th, July 15th, October 15th, and January 15th).

Annual Inspections:

RAP will conduct an audit of the TRUST Ordinance technologies in combination with their annual Departmental audits, which will include:

1. Confirmation of the managing units' audits/inspections and data collection.

2. Conducting an independent audit/inspection on items, such as the equipment/software as well as their access and use, that have not previously been inspected by the managing unit's quarterly inspections.

These audits/inspections will be documented in the RAP Unit annual inspection memo that is presented to the Deputy Chief for review and approval.

These audits/inspections will be in addition to any unit inspections that are deemed necessary by the commanding officer of each unit or the Chief of Police.

Data Breaches:

If a Department member becomes aware of a data breach during business hours, they shall **immediately** notify the Information Technologies Unit to begin securing the breach and assessing the intrusion or compromise to the Department data. The Information Technology Unit will contact RAP and report the data breach, along with the steps being taken to stop the breach.

If the breach is detected after hours, the discovering Department member shall **immediately** notify the Help Desk at **(Redacted - record exempt)**, who will notify the on-call Information Technology member of the breach. The Information Technology Unit will notify RAP of the breach for documentation purposes.

Improper Use:

If a Department member becomes aware of improper use of an approved technology, they shall notify their supervisor. The supervisor shall notify the managing unit for the technology, who shall review the issue and determine the next course of action (e.g. training, disciplinary investigation, etc.). The RAP Unit shall be notified of the improper use of the technology by the managing unit, and what the next course of action will be.

If you have any questions, please contact the RAP Unit, **(Redacted - record exempt)**.

Please read at squad conferences and give a copy to all personnel.