The City of SAN DIEGO

**Privacy Advisory Board**

# A Guide for Complying with the TRUST Ordinance

City of San Diego

Privacy Advisory Board

March 2026
Version 1.0

The City of SAN DIEGO

# Privacy Advisory Board

## TABLE OF CONTENTS

**Page**

The City of SAN DIEGO

# Privacy Advisory Board

## Introduction

The following is a guide on how to comply with the City of San Diego's Transparent and Responsible Use of Surveillance Technology ("TRUST") Ordinance (S.D. Municipal Code section 210.0101, *et seq*.) The TRUST Ordinance requires all City departments, divisions, agencies, and committees[1] to report on specific topics and to create policies to ensure that all City entities using "surveillance technology" comply with the Ordinance's goals. It requires the production of a Surveillance Impact Report and Surveillance Use Policy for each new and existing surveillance technology, along with an Annual Surveillance Report on every surveillance technology an agency owns. Templates for each of these reports are attached to this Guide as exhibits A, B, and C, respectively. To ensure consistent and reliable reporting, the Privacy Advisory Board urges you to follow these templates. This Guide provides detailed explanations for each type of report for how to respond to each category of required information and how to obtain approval for a surveillance technology under the TRUST Ordinance.

In today's digital world, vast amounts of personal information are collected and stored for many purposes. Governments hold large quantities of personal data which, if shared or stolen, can be exploited for personal gain, criminal activity, or commercial use in the "data economy" without an individual's knowledge or informed consent. The TRUST Ordinance seeks to protect individuals from privacy violations, identity theft, and infringements on civil rights and liberties that can result from data breaches, misuse or overuse of information, and inadequate data protection.

Technology can offer a cost-effective way to maximize a city's efforts to deliver services and meet various expectations. The TRUST Ordinance provides a framework for evaluating whether a surveillance technology is worth its risks and how to minimize those risks. Through the TRUST Ordinance, the Privacy Advisory Board and City departments can fulfill government's first mission: protecting its residents and visitors.

If you have questions about compliance with the TRUST Ordinance do not hesitate to reach out. If you have suggestions on how we can assist in making TRUST Ordinance compliance easier and more effective, we welcome your feedback.

---

[1] For ease of reference, departments, divisions, agencies, and committees subject to the TRUST Ordinance are referred to as a "department."

# TRUST Ordinance Table of Contents

The following is a table of contents for the TRUST Ordinance. All references are to Chapter 2, Article 10 of the San Diego Municipal Code.

# Some Preliminary Concepts

The TRUST Ordinance creates a process by which surveillance technology is evaluated before it is procured and a process to follow to ensure continued compliance with the ordinance. The Surveillance Use Policy sets out the rules governing how a surveillance technology will and will not be used to ensure that sensitive data is protected. The Surveillance Impact Report is used to evaluate the surveillance technology and measures that will be taken to protect sensitive data. It is created before a surveillance technology is approved for use. Finally, the Annual Surveillance Report reviews the effectiveness of an approved surveillance technology and its safeguards. As the name suggests, it is created and presented to the Privacy Advisory Board each year.

Your department may have existing processes for contracts, procurement, vendor retention, technology management, information security, and data governance. These processes may be useful in preparing the reports required under the TRUST Ordinance.

In complying with the TRUST Ordinance, the following should be taken into account:

## Accountability

- Incorporate the TRUST Ordinance requirements into the procurement process for a new surveillance technology
- Assign reporting and policymaking to more than one individual if appropriate. Consider someone from contract, vendor, or technology management and someone with sufficient authority
- Consider creating a training curriculum to prevent misuse of surveillance technology and data

## Transparency

- Surveillance Use Policies, Surveillance Impact Reports, and Annual Surveillance Reports are required for every surveillance technology and must be publicly available (§210.0106(b)(c))
- Before presenting a surveillance technology to the Privacy Advisory Board for review, the TRUST Ordinance requires each department to hold at least one publicly noticed community meeting in each council district in which the surveillance technology will be used. (§210.0103)

- Gather information about public records requests concerning the surveillance technology such as the number of requests, response times, types of information requested and released
- Track community engagement about the surveillance technology
- Build a model for obtaining data and calculating relevant statistics on surveillance technologies
    - technological, organizational, and administrative costs
    - effectiveness in meeting the purpose of the surveillance technology
- Disclose all surveillance technology contracts, including all related non-disclosure agreements to the extent permitted by law (§210.0110)
- Prepare for closed session meetings with City Council, where necessary, on cybersecurity risks (§210.0108 (d))

## Technology Management and Auditing

- Auditing and Oversight Measures Are Essential (§210.0108)

  Auditing and oversight measures are how one ensures compliance with rules. They are invaluable in detecting issues before the issues become problems. At a minimum, an audit and inspection program should contain the following:

    - Clear documented policies and procedures that are always followed, not general guidelines that are followed only when convenient.
    - A way to tie the risk to the control to the audit test. The following chart is a sample Risk Control Matrix to assist you. For every risk identified with the surveillance technology, include at least one Mitigation and one Test of Control/Audit Step:

| **Sample Risk and Control Matrix for City Departments** | | |
|---|---|---|
| **Identified Risk (What could go wrong?)** | **Core Control Process (Mitigation)** | **Audit Step (Test of Control)** |
| Unauthorized access to program or configure the surveillance technology | Granting system access only on restricted servers | Authorized system users are compared to Department employment records and only approved personnel are included |
| | System vendor restricts access to programs authorized by Department | Test that vendor has surveillance technology settings agreed upon by Department (and not set to |

| Sample Risk and Control Matrix for City Departments | | |
|---|---|---|
| | | default settings) |
| | | Vendor obtains six month audits from outside vendors of its service center controls |
| Specific use of technology not authorized by City of San Diego | Require a valid incident/citation number to access | Ensure program will not advance without traceable incident/citation number |
| Databases are not kept longer than the legal retention limits | System is programed to purge data after set number of days | Review data at point in time to ensure that no data is older than the authorized threshold |

  - The person conducting the audit/inspection should be independent of the staff members you are inspecting. In most cases, the auditor should not be a supervisor.
  - Make sure all risks are covered, including vendor risks. The department is responsible for managing the vendor.
  - Ensure there is a planned and formal inspection scope/sample size. A sample size will then be able to infer the accuracy of the overall population.
  - Track findings and analyze them regularly to determine trends and root causes of any problems. When an issue is found, it should not be treated as an exception or "one-off" and dismissed. The identified issue must be extracted to the population and understood so it can be corrected and avoided in the future. Seemingly isolated issues can lead to large problems.
  - Personnel who are responsible for an issue or deviation from a policy should be held accountable.
  - Audits must be documented. When properly done, an audit can be replicated by a third party.
- Documentation (Annual Surveillance Report and Surveillance Impact Report)
  - Track general and specific (individual) uses of surveillance technology
  - Track access to data collected by surveillance technology, track the number and nature of all disclosures
  - Take account of data and physical hardware location(s)

  - Data Lifecycle and Mapping: What kinds of personal data at collected? What kinds of relevant non-personal data exist? Where is the data collected from? Where and how is it being sent? What is the specific use for the data and has that specific use been reviewed by the Privacy Advisory Board and approved by the City Council? How long will the data be stored, either by the City or trusted third-parties? Does the data need to be stored for that long? What is the legal basis for storing the data? What privacy and cybersecurity protections exist? What happens to the data and technology once it is no longer used or the contract ends?
- Anticipate Issues
  - Anticipate possible legal, ethical, and privacy risks
  - Perform a periodic review of the Surveillance Impact Report checking whether risks have remained accurate
  - Gather reports on the effects of your surveillance technologies in other cities or municipalities

# Approval Process

## Privacy Advisory Board Review Process

This section discusses the Privacy Advisory Board review process of new and existing surveillance technology. *See* §§210.0104 and 210.0105.

Before September 9th, 2026, existing Surveillance Technology may be used under existing contracts. City staff must submit a comprehensive list of existing Surveillance Technology in its possession or use. After submitting the comprehensive list, City staff have 60 calendar days to submit at least one notification memo, the Surveillance Use Policy and the Surveillance Impact Report each month for the Privacy Advisory Board's review and recommendation until all surveillance technologies on the list have been reviewed. The Privacy Advisory Board will rank the existing surveillance technology in order of potential impact and review each technology.

Surveillance technology (new and existing) on or after September 9th, 2026, must go through the following review process: In preparation for the delivery of a Surveillance Use Policy, each department must hold at least one publicly noticed community meeting (§210.0103). Following the meeting, send a memo providing the Surveillance Impact Report

and the Surveillance Use Policy before soliciting proposals for surveillance technology or implementing Surveillance Technology jointly with another City department (§210.0104). Finally, the Privacy Advisory Board will either recommend to City Council the acquisition of the Surveillance Technology, recommend with modifications to the Surveillance Use Policy, object to the proposed Surveillance Use Policy, or offer no recommendation. If the Board does not take action on a new or existing surveillance technology within 90 calendar days after the Board Chair is notified by Memorandum, City Staff may proceed to City Council for approval (210.0104(e) and 2010.0105(g)).

## City Council Approval Process

City Council approval is required before a) accepting donations for surveillance technology, b) acquiring surveillance technology (including without consideration), and c) using surveillance technology (new or existing) for a purpose or in a location not described in a City Council-approved Surveillance Use Policy (§210.0106(a)). Once the Board has reviewed the reports (or after 90 days without action), request a date with City Council for their consideration of the surveillance technology. The City Council will use the approval standard below, and the City Council may modify the Surveillance Use Policy if necessary to meet the standard. If City Council's approval has not been given within four City Council meetings since initially considering the existing Surveillance Technology, City agencies must stop using it. (§210.0106(b)(5)).

City Council Approval Standard (§210.0106(b)(2)): a) Benefits to the community outweigh the costs, b) the Surveillance Technology will safeguard civil rights and liberties, and c) there is no effective alternative that provides a less financial cost and impact on civil rights and liberties.

## After City Council Approval

After City Council approves of the surveillance technology and its Surveillance Use Policy, City staff must submit an Annual Surveillance Report of surveillance technology approved on or after January 1 of the prior year by February 1 for as long as the surveillance technology is in use. For example, if a surveillance technology is approved in August 2026, then an Annual Surveillance Report should submitted to the Privacy Advisory Board and to City Council by February 1, 2027; surveillance technologies approved in December 2025 will need an Annual Surveillance Report in February 2026. The Privacy Advisory Board will provide recommendations and City Council will approve of the continued use of the surveillance technology. If the Privacy Advisory Board does not provide a recommendation

within 90 days of receiving the Annual Surveillance Report, then city staff may seek approval from City Council on whether the Surveillance Use Policy should remain in effect. City staff may also have a closed meeting with City Council to discuss cybersecurity risks (§210.0108).

### Guidance on the Surveillance Impact Report and Surveillance Use Policy

Develop the Surveillance Impact Report and the Surveillance Use Policy concurrently. The two documents are just as much about reporting as they are about educating yourself about privacy and civil rights risks associated with the surveillance technology. You may want to add more safeguards for the data collected as you learn about negative impacts or ways in which data might be at risk. Additionally, some topics of the Impact Report (4 & 7) are about the Use Policy so doing them concurrently will assist with the prompt completion of both.

The process for completing these two documents should be similar to this: find all the facts about the surveillance technology (its purpose, use, data, hardware, software, statistics, etc.), think of the current protections (technical, administrative, organizational), analyze how it might affect community (impacts, rights, liberties, trust, privacy), then finally amend protections to address discovered risks. Once these documents are drafted, the Privacy Advisory Board will review them for thoroughness, completeness, and consistency. We'll be in conversation with City departments/agencies in case the report or policy needs more attention.

## Annual Surveillance Report

The following tracks the information the TRUST Ordinance requires to be included in the Annual Surveillance Report and provides a description of the requested information.

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

   This asks about the purposes of each surveillance technology used— include the general purpose (e.g., public safety, security, fleet management, waste prevention) and a more descriptive purpose or outcome such as to prevent unauthorized personnel from entering an area or to collect analytics.

   You should include all types of information gathered or analyzed, and the amount of the data gathered or analyzed. For example, a camera may capture

images of people, or a web portal may gather names, addresses, dates of birth, medical information, and payment information provided by those accessing the portal.

Some or all the data may be collected by your department or provided from another City department or an outside source. Regardless of the source of the data, you should include it in your department's Annual Surveillance Report.

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.

   This requests information about how and when you shared data with non-City entities of any type for any purpose. It includes formal, routine sharing as well as informal sharing, such as when someone calls and asks your department for information.

   The request also asks for the authority, legal standard, or justification for sharing the information, if any. Since the information at issue is personal consumer information, a City entity generally should not share that information outside of the City without authorization. Because of the way even small, seemingly insignificant pieces of personal information now can be aggregated and analyzed in ways never previously available, a primary goal of the TRUST Ordinance is to ensure that data is shared only when authorized to ensure everyone's personal information is protected.

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.

   This asks for a description of the object the hardware may be attached to (may not apply to software only surveillance tools). For example, automatic license plate readers tend to be attached to streetlights. Surveillance cameras may be attached to buildings, electrical poles, trees, or vehicles.

Secondly, describe how the hardware or software obtained its data. That is, the source of collected data. Data can be obtained either through the different kinds of hardware sensors (e.g., Pan-Tilt-Zoom camera, 360 camera, infrared camera, microphones) or from an identifiable data sink, data sharing agreement with, or some collection process (internally or externally). Data can be collected through web portals, at kiosks, or from forms filled out by people using City services.

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.

   Include in this section all updates or changes, and the reason for doing so. For example, an upgraded camera may have greater resolution and zoom capabilities, a software system may connect to a greater software system, or even where a software system is processing data related to a greater variety of people. Include changes that may or may not have been initiated by the department, as any change of this kind could increase privacy risks. The vendor who supplied the technology may provide software or hardware upgrades.

   If you do not know whether a vendor or someone else provided any software updates, hardware upgrades, or system configuration changes, contact the vendor or other responsible party to find out. In the past, the City department might have left it to a vendor to maintain surveillance technology without closely monitoring any changes. This is no longer acceptable practice, as reflected in the TRUST Ordinance requirements.

5. A description of where the surveillance technology was deployed geographically, by each City Council District or police area, in the applicable year.

   Include general descriptions of technology location. If the surveillance technology is software, describe generally those individuals who may be surveilled or whose information may be collected by their geographic location.

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.

    This seeks information that can play an important role in assessing whether a technology is being properly used or the data collected is sufficiently protected.

    Different people or groups of people have differing views on the collection of information about them and the extent of collection. For example, some communities may believe they are "over-policed." Some groups may believe they are harassed when obtaining government benefits or engaging in civic activities.

    This question contains two parts. First, have any complaints or concerns been expressed about a technology or the scope of its use? Complaints and concerns may be expressed formally or informally and can be made at different times and places, such as complaints to a City department, at a community meeting, through the media, or otherwise. If available, a tabulation of complaints and concerns should be provided. A description of less formal methods of complaints should also be provided.

    The question also seeks information about whether certain groups or individuals are disproportionately impacted. This information should be provided regardless of whether the impact is justified.

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.

    Include in this section audit results and your agency response to them (if applicable). For example, an audit may have revealed that data may have been shared, or the technology was used in a way misaligned with the Surveillance Use Policy. Describe the response.

Generally, any City entity using surveillance technology should audit its use to ensure that use is consistent with the technology's Use Policy. The audit may not be formal and may not need to be especially detailed but should still be included in response to this question.

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.

   This question seeks information about data breaches and other forms of unauthorized access to data. One way to view unauthorized access is access to data that is not permitted by the technology's Use Policy. Both data breaches and other types of unauthorized access should be reported.

   A breach or other unauthorized access includes any unauthorized access to the data even if nothing is done once accessed, as well as unauthorized sharing, viewing, duplication, deletion, or other processing of data. Encrypted data that was improperly accessed should be included in this section.

   The scope and response to a breach or unauthorized access should be explained.

   For many surveillance technologies, the database is held and maintained by someone other than the City. For example, the vendor may store the data, or the data may be in a cloud-based storage operated by a third party. Regardless of where the data is stored, any breach or unauthorized access should be included. If the data is held by a third party, you will need to contact the third party to adequately respond to this request.

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.

This section asks about methodologies you have in place to detect data breaches or other access by someone not authorized to access the data. The response may include information about audits or breach detection software. If no such measures are in place, please state that explicitly.

You should not provide detailed information that would assist a data thief committing a breach or preventing the detection of a breach. If you have any concerns that a proposed answer may do this, you should contact the City's data security official.

10. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes.

    This question seeks information to help assess whether the surveillance technology is useful to the City to achieve the reason for the technology. There are many ways to assess whether a technology fulfills the purpose for having the technology. Depending on its use, there may be statistics that are gathered and analyzed. Other times, a description of how it improves one's work, or makes that work easier or less costly is sufficient. Consider a wide range of factors relevant to the technology's use, such as operational costs, investigation impact, public interest, technological effectiveness, or data quality.

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.

    Include statistics and information on California Public Records Act requests. Include (if applicable) any insights or notes on information about the surveillance technology shared via the public records act.

    In addition to the number of requests made, response rates, open and close dates, and similar information, include information about the type of information that is provided in response to the public records act request. Responses to public records act requests can be a source of information privacy loss. Responding to this request provides an opportunity to evaluate

whether personal information is being shared in response to a public records act request.

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.

    This question asks for a comprehensive assessment of the annual costs for a surveillance technology and all their funding sources. This request seeks information beyond only the cost of the technology itself.

13. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request.

    You may find that a surveillance technology could be useful for something more than set for in the Surveillance Use Policy. You may also find that use of the technology in accordance with the Surveillance Use Policy nonetheless leads to or may lead to a violation of one's privacy rights, civil rights or civil liberties. In either case, a modification of the technology's Surveillance Use Policy may be appropriate. Your suggested modifications will help the City provide better service to its residents while protecting their privacy, civil liberties, and civil rights.

## Surveillance Impact Report

The following tracks the information the TRUST Ordinance requires to be included in the Surveillance Impact Report.

1. Description: Information describing the surveillance technology and how it works, including product descriptions from manufacturers, if available.

   Describe the surveillance technology as a technology; that is, describe how it works, product descriptions, deviations from commercial technology, or other analyses.

2. Purpose: Information on the proposed purposes and outcomes for the surveillance technology.

This should answer the question of why the surveillance technology was acquired or why the surveillance technology should be acquired. Describe the issue the surveillance technology is meant to solve, its projected outcomes, and what the technology is meant for.

3. Location: The physical or virtual locations where the surveillance technology may be deployed, using general descriptive terms and crime statistics for the locations.

   The locations of surveillance technology allow the City to assess its impact.

4. Impact: An assessment of the Surveillance Use Policy for the particular surveillance technology, including whether there is adequate protection of civil rights and civil liberties and whether the surveillance technology may be used or deployed, intentionally or inadvertently, in a manner that may disproportionately affect marginalized communities.

   This section is about risks and protections from harm based on the proposed Surveillance Use Policy. Harm as described above is the inadequate protection of civil rights, civil liberties, or an inequitable impact. For example, a surveillance camera system may be installed in areas with a population of at a historically lower socioeconomic level, or those who benefit from the use of a surveillance technology is made up of a single group, or simply personal information collected from a surveillance technology is being shared indiscriminately.

   Consider performing this section last along with “Mitigation” after going through the other sections, since more than half of the process is fact gathering, while sections like this one makes the report writer analyze. If you find possible negative impacts, mitigate them (propose mitigations) though technical, administrative, or other means, and then detail the mitigations in Data Security (7) or Mitigations (5).

   See FAQ for more information on Rights, Liberties, and Impacts.

5. Mitigation: Identification of specific, affirmative technical and procedural measures that will be implemented to safeguard the public from each identified impact.

Describe the measures used to safeguard civil rights, civil liberties, and inequitable impact. Consider whether it is appropriate (or ethical) to deploy surveillance technologies on people.

6. Data Types and Sources: A list of all types and sources of data to be collected, analyzed, or processed by the surveillance technology, including scores, reports, the logic or algorithm used, and any additional information derived from the surveillance technology, 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.

   Data Source refers to where the data came from; not only from hardware and software collection vectors but from technology like artificial intelligence and machine learning, that can make inferences, generate probable knowledge, or analyze and aggregate other kinds of data.

7. Data Security: Information about the controls that will be designed and implemented to safeguard the data collected or generated by the surveillance technology from unauthorized access or 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.

   Describe the security posture of the surveillance technology and data without offering compromising information about it.

8. Fiscal Cost: The forecasted, prior, and ongoing fiscal costs for the surveillance technology, if known and available, including known or projected initial purchase costs, personnel costs, and other ongoing costs, and any current or potential sources of funding.

   Financial cost play a role in determining whether the benefits outweigh the costs.

9. Third Party Dependence: Whether use or maintenance of the surveillance technology will require data gathered by the surveillance technology to be handled or stored by a third-party vendor at any time.

   This offers the City an idea of the risks related to third-party data breach, third-party data sharing, and third-party misuse.

10. Alternatives: A summary of the alternative means to achieve the proposed purposes considered, including alternative means that do not involve the use of surveillance technology, before deciding to use the proposed surveillance technology, including the costs and benefits associated with each alternative considered and an explanation of the reasons why each alternative is inadequate or less effective.

    Surveillance technology can often maximize effort, optimize time, or save money; however, they are rarely the only method to achieve a certain goal or solve a problem. Consider alternatives to surveillance technology such as physical security, policy, employees, or less "smart" technology. For example, the cost of a surveillance technology could include civil rights, civil liberty, inequitable impacts, legal issues, societal harm, loss of trust from the community, or invasions of privacy.

11. Track Record: A summary of the experience, if any, of other entities, especially government entities, with the proposed surveillance technology, including, if available, quantitative information about the effectiveness of the proposed surveillance technology in achieving its stated purpose in other jurisdictions and any known adverse information about the surveillance technology, such as unanticipated costs, failures, or abuses of civil rights or civil liberties, existing publicly reported controversies, and any court rulings in favor or in opposition to the surveillance technology.

    Present research on the proposed or current surveillance technology having been used in other government entities. Consider sources external to the target government entity and cite sources giving a general idea of the history and impact of the technology in other communities.

12. Public Engagement and Comments: A description of any community engagement held and any future community engagement plans, number of attendees, and compilation of all comments received and City departmental responses given, and City departmental conclusions about potential neighborhood impacts and how the impacts that may result from the acquisition and use of the surveillance technology may differ as they pertain to different members of the community.

    To obtain approval for surveillance technology, the City will need to hold at least one publicly noticed community event per section 210.0103. Include in this section descriptions of any community engagement including community

events. Capture as much information about how community members view the technology or its uses, both positive and negative. Community concerns can often be addressed through stricter data control and protection.

## Surveillance Use Policy

The following tracks the information the TRUST Ordinance requires to be included in the Surveillance Use Policy.

1. Purpose: The specific purposes that the surveillance technology is intended to advance.

   Describe the purpose of the surveillance technology; what issues will it help resolve or what benefits will come about from using it.

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.

   Describe how the surveillance technology will be used, include any rule or process required for its use. For instance, drones may be used to inspect buildings at great heights, and drone pilots must first have completed training and obtain a license to fly it.

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.

   List all the ways in which information, especially personal information, is collected include data sources that the technology will rely upon such as sensors, joint data pools, surveys, or other methods of collection. Also include ways in which you intend to minimize the collection of information and limit how long you hold onto that data.

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.

    Who will be able to access personal information or data collected by the surveillance technology?

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.

    Describe the ways in which you plan on protecting personal information or information collected by the surveillance technology. Sensitive personal information like Social Security numbers may need to be encrypted; names can be hashed for pseudonymization; transfer protocols may be encrypted.

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.

    Consider referencing City data retention standards, and where none exist, consider limiting the retention period to the minimum necessary; include the reason a retention time is appropriate, the deletion processes, and any reason why information is held beyond a certain period. For example, consider a case where the City conducts a service for a group of people where names and contact information are essential for financial reporting or compliance with grants. The information should be retained for as long as required for the purposes, but not longer.

7. Public Access: A description of how collected information can be accessed or used by members of the public, including criminal defendants.

Some City departments may have open data portals or other avenues for the public to view data. Describe any applicable public access vector.

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 that information.

   Detail all the ways in which data is shared with third parties. Mention contracts related to the data sharing along with notable clauses such as if a data breach occurs, the third-party will notify the City as soon as possible.

9. Training: The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology.

   Consider training authorized individuals to prevent misuse, unauthorized data sharing, or other policy in the Surveillance Use Policy. For example, individuals with a license to pilot a drone may be trained to avoid flying over people's homes or record video only when necessary; or an individual who has access to personal information could be trained on the prohibited data sharing aspects of a Surveillance Use Policy.

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.

    How will you ensure that the Surveillance Use Policy will be followed? As the Ordinance suggests, consider putting people in charge of department compliance, developing internal recordkeeping processes, employing an independent agent for oversight, and developing sanctions for violations. Consider increased training on proper technology and information use and technical safeguards.

11. Maintenance: The procedures used to ensure that the security and integrity of the surveillance technology and collected information will be maintained.

    What measures are in place to ensure that the technology will continue to work as intended, that software is kept up-to-date, and that security protocols are maintained? What about security for Application Programming Interfaces (APIs)? How will data quality and protection be maintained?

# FAQ

Q: What is the Privacy Advisory Board?

A: The Privacy Advisory Board was established by the Council of the City of San Diego in Ordinance O-21446, effective May 12, 2022, codified in San Diego Municipal Code Chapter 2, Art. 6, Div. 00, Sec. 26.42, and Sec. 26.43 which states: It is the purpose and intent of the Council to establish a Privacy Advisory Board to serve as an advisory body to the Mayor and Council on policies and issues related to privacy and surveillance. The board will provide advice intended to ensure transparency, accountability, protection of rights, and public deliberation in the City's acquisition and use of surveillance technology. https://www.sandiego.gov/pab.

Q: What about surveillance technology before Sept. 6, 2026?

A: Before September 9, 2026, City staff may continue to use existing surveillance technology, under existing contracts, contract amendments, or contract options, or new contracts entered into under the City's procurement processes, without seeking the Board's advisory review and recommendation related to the existing surveillance technology or City Council review of a Surveillance Impact Report and approval of a Surveillance Use Policy. This grace period allows City staff and the Board to fully implement the necessary procedures to comply with this Division (see §210.0105 (a)).

Q: What about surveillance technology after Sept. 6, 2026?

A: After this date, City agencies must obtain City Council approval to obtain surveillance technology and continue using existing surveillance technology. In obtaining City Council approval, departments must create a Surveillance Use Policy and Surveillance Impact Report for review by the Privacy Advisory Board.

Q: When should we send the Annual Surveillance Report to the Privacy Advisory Board?

A: The deadline to submit the Annual Surveillance Report is February 1 of the following year. For example, a report meant to address surveillance technology in 2026 will have a deadline of February 1, 2027 (see §210.0108 (a)).

Q: Will every proposed surveillance technology need a Surveillance Use Policy and Surveillance Impact Report?

A: Yes, new and existing after September 2026.

Q: Do you have any examples or templates of these required documents?

A: Take a look at the Privacy Advisory Board's website for the SDPD Surveillance Impact Report, Surveillance Use Policy, and Annual Surveillance Report as guidance or as a kind of template.

Q: What do you mean by civil rights, civil liberties, and inequitable impacts?

A: Civil rights refer to the protections and privileges that ensure individuals are treated equally and fairly under the law. They focus on preventing discrimination and ensuring equal access to opportunities, such as voting, education, and employment. While, civil liberties are the basic freedoms and protections from government interference, ensuring individuals can act according to their own choices, free from government oppression. For example, the right to privacy, freedom of speech, and freedom of religion. In short, civil rights are about equality and non-discrimination, while civil liberties are about protecting individual freedom. Inequitable impacts refer to inequitable benefits or harms stemming from the employment of surveillance technology.

Q: The surveillance technology we use was approved, but we want to change aspects of it that may change its risk profile. What do we do?

A: City Council may need to approve of a change; connect with the PAB for review §210.0106 (3). See also Annual Surveillance Report part 13 which allows requests for modifications to the Surveillance Use Policy.

Q: What if our City department needs to use a surveillance technology immediately without approval?

A: see §210.0107 on the use of unapproved surveillance technologies for exigent circumstances, that is, an emergency involving danger of death or serious physical injury to

any natural person, or imminent danger of significant property damage, that requires surveillance technology determined by city staff in good faith.

Additional Questions?

Tim Blood, Chair, Privacy Advisory Board
tblood@bholaw.com

# Exhibit A

# Surveillance Impact Report

[INSERT NAME OF SURVEILLANCE TECHNOLOGY]

[INSERT NAME OF CITY/DEPARTMENT/AGENCY]

## DESCRIPTION:

Information describing the *surveillance technology* and how it works, including product descriptions from manufacturers, if available.

[Insert Response]

## PURPOSE:

Information on the proposed purposes and outcomes for the *surveillance technology*.

[Insert Response]

## LOCATION:

The physical or virtual locations where the *surveillance technology* may be deployed, using general descriptive terms and crime statistics for the locations.

[Insert Response]

## IMPACT:

An assessment of the *Surveillance Use Policy* for the particular *surveillance technology*, including whether there is adequate protection of civil rights and civil liberties and whether the *surveillance technology* may be used or deployed, intentionally or inadvertently, in a manner that may disproportionately affect marginalized communities.

[Insert Response]

# Surveillance Impact Report

[INSERT NAME OF SURVEILLANCE TECHNOLOGY]

[INSERT NAME OF CITY/DEPARTMENT/AGENCY]

## MITIGATION:

Identification of specific, affirmative technical and procedural measures that will be implemented to safeguard the public from each identified impact.

[Insert Response]

## DATA TYPES AND SOURCES:

A list of all types and sources of data to be collected, analyzed, or processed by the *surveillance technology*, including scores, reports, the logic or algorithm used, and any additional information derived from the *surveillance technology*, 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*.

[Insert Response]

## DATA SECURITY:

Information about the controls that will be designed and implemented to safeguard the data collected or generated by the *surveillance technology* from unauthorized access or 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*.

[Insert Response]

# Surveillance Impact Report

[INSERT NAME OF SURVEILLANCE TECHNOLOGY]

[INSERT NAME OF CITY/DEPARTMENT/AGENCY]

## FISCAL COST:

The forecasted, prior, and ongoing fiscal costs for the *surveillance technology*, if known and available, including known or projected initial purchase costs, personnel costs, and other ongoing costs, and any current or potential sources of funding.

[Insert Response]

## THIRD PARTY DEPENDENCE:

Whether use or maintenance of the *surveillance technology* will require data gathered by the *surveillance technology* to be handled or stored by a third-party vendor at any time.

[Insert Response]

## ALTERNATIVES:

A summary of the alternative means to achieve the proposed purposes considered, including alternative means that do not involve the use of *surveillance technology*, before deciding to use the proposed *surveillance technology*, including the costs and benefits associated with each alternative considered and an explanation of the reasons why each alternative is inadequate or less effective.

[Insert Response]

# Surveillance Impact Report

[INSERT NAME OF SURVEILLANCE TECHNOLOGY]

[INSERT NAME OF CITY/DEPARTMENT/AGENCY]

## TRACK RECORD:

A summary of the experience, if any, of other entities, especially government entities, with the proposed *surveillance technology*, including, if available, quantitative information about the effectiveness of the proposed *surveillance technology* in achieving its stated purpose in other jurisdictions and any known adverse information about the *surveillance technology*, such as unanticipated costs, failures, or abuses of civil rights or civil liberties, existing publicly reported controversies, and any court rulings in favor or in opposition to the *surveillance technology*.

## PUBLIC ENGAGEMENT AND COMMENTS:

A description of any community engagement held and any future community engagement plans, number of attendees, a compilation of all comments received and *City* departmental responses given, and *City* departmental conclusions about potential neighborhood impacts and how the impacts that may result from the acquisition and use of the *surveillance technology* may differ as they pertain to different members of the community.

# Exhibit B

# Surveillance Use Policy

[INSERT NAME OF SURVEILLANCE TECHNOLOGY]

[INSERT NAME OF CITY/DEPARTMENT/AGENCY]

## PURPOSE:

The specific purposes that the *surveillance technology* is intended to advance.

[Insert Response]

## 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.

[Insert Response]

## DATA COLLECTION:

The information that can be collected, captured, recorded, intercepted, or retained by the *surveillance technology*, data that may be inadvertently collected during 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*.

[Insert Response]

# Surveillance Use Policy

[INSERT NAME OF SURVEILLANCE TECHNOLOGY]

[INSERT NAME OF CITY/DEPARTMENT/AGENCY]

## 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*.

[Insert Response]

## DATA PROTECTION:

The safeguards that protect information from unauthorized access, including system logging, encryption, and access control mechanism, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security of the *City*.

[Insert Response]

## DATA RETENTION:

The time period, if any, for which information collected by the *surveillance technology* will be routinely retained, the reason that 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.

[Insert Response]

# Surveillance Use Policy

[INSERT NAME OF SURVEILLANCE TECHNOLOGY]

[INSERT NAME OF CITY/DEPARTMENT/AGENCY]

## PUBLIC ACCESS:

A description of how collected information can be accessed or used by members of the public, including criminal defendants.

[Insert Response]

## 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.

[Insert Response]

## TRAINING:

The training required for any individual authorized to use the *surveillance technology* or to access information collected by the *surveillance technology*.

[Insert Response]

## 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.

[Insert Response]

# Surveillance Use Policy

[INSERT NAME OF SURVEILLANCE TECHNOLOGY]

[INSERT NAME OF CITY/DEPARTMENT/AGENCY]

## MAINTENANCE:

The procedures used to ensure that the security and integrity of the *surveillance technology* and collected information will be maintained.

[Insert Response]

# Exhibit C

# [YEAR] Annual Surveillance Report

[INSERT NAME OF SURVEILLANCE TECHNOLOGY]

[INSERT NAME OF CITY/DEPARTMENT/AGENCY]

## DESCRIPTION OF USE AND DATA:

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

[Insert Response]

## DATA SHARING AND JUSTIFICATION:

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*.

[Insert Response]

## DESCRIPTION OF SURVEILLANCE TECH:

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.

[Insert Response]

# [YEAR] Annual Surveillance Report

[INSERT NAME OF SURVEILLANCE TECHNOLOGY]

[INSERT NAME OF CITY/DEPARTMENT/AGENCY]

## UPDATES AND UPGRADES:

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*.

[Insert Response]

## LOCATION:

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

[Insert Response]

## COMMUNITY COMPLAINTS:

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.

[Insert Response]

# [YEAR] Annual Surveillance Report

[INSERT NAME OF SURVEILLANCE TECHNOLOGY]

[INSERT NAME OF CITY/DEPARTMENT/AGENCY]

## AUDIT OR INVESTIGATION RESULTS:

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.

[Insert Response]

## DATA BREACHES:

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*.

[Insert Response]

## DATA BREACH DETECTION METHODOLOGY:

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*.

[Insert Response]

# [YEAR] Annual Surveillance Report

[INSERT NAME OF SURVEILLANCE TECHNOLOGY]

[INSERT NAME OF CITY/DEPARTMENT/AGENCY]

## EFFECTIVENESS:

Information, including crime statistics, that helps the community assess whether the *surveillance technology* has been effective at achieving its identified purposes.

[Insert Response]

## PUBLIC RECORDS REQUESTS:

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.

[Insert Response]

## FISCAL 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.

[Insert Response]

## REQUESTED MODIFICATIONS:

Any requested modifications to the *Surveillance Use Policy* and a detailed basis for the request.

[Insert Response]