City & County of San Francisco

The City Should Consider Risk-Based Monitoring of Surveillance Technology

Office of the City Administrator

Why It Matters

The Committee on Information Technology and city departments have made progress in implementing the City's Acquisition of Surveillance Technology Ordinance. However, 31 technologies in use when the law passed in 2019 still do not have approved use plans. Where the law applies, it treats all technologies the same, regardless of how much or how little they may affect city residents' privacy, so the City may be wasting resources by closely monitoring low-risk uses. Also, the law applies inconsistently across criminal justice departments. The City will continue to have gaps in its privacy protections until the law is amended to enable complete, risk-based oversight and compliance monitoring.

Prepared by

OFFICE OF THE CONTROLLER
CITY SERVICES AUDITOR

October 8, 2025

About the Controller's Office

The Controller is the chief financial officer and auditor for the City and County of San Francisco. We produce regular reports on the City's financial condition, economic condition, and the performance of City government. We strive to be a model for good government and to make the City a better place to live and work.

About the Audits Division

The City Services Auditor (CSA) was created in the Office of the Controller through an amendment to the Charter of the City and County of San Francisco (City) that voters approved in 2003. Within CSA, the Audits Division ensures the City's financial integrity and promotes efficient, effective, and accountable government by:

- Conducting performance audits of city departments, contractors, and functions to assess efficiency and effectiveness of service delivery and business processes.
- Investigating reports received through its whistleblower hotline of fraud, waste, and abuse of city resources.
- Providing actionable recommendations to city leaders to promote and enhance accountability and improve the overall performance and efficiency of city government.

Team:

Amanda Sobrepeña, *Lead Audit Manager*
Kat Scoggin, *Audit Manager*
Hunter Wang, *Audit Manager*
Jessica Runzel, *Staff Auditor*
Bryanna Shu, *Staff Auditor*

For more information, please contact:
Mark de la Rosa
Director of Audits
(415) 554-7574

Media inquiries:
con.media@sfgov.org

sf.gov/controller
@sfcontroller
Controller's Office LinkedIn

AUDIT AUTHORITY

This audit was conducted under the authority of the San Francisco Charter, Section 3.105 and Appendix F, which requires that CSA conduct periodic, comprehensive financial and performance audits of city departments, services, and activities.

STATEMENT OF AUDITING STANDARDS

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the findings and conclusions based on our audit objectives. The Audits Division is independent per GAGAS requirements for internal auditors.

OFFICE OF THE CONTROLLER
CITY AND COUNTY OF SAN FRANCISCO

Greg Wagner
Controller

ChiaYu Ma
Deputy Controller

October 8, 2025

Board of Supervisors
City and County of San Francisco
City Hall, Room 244
1 Dr. Carlton B. Goodlett Place
San Francisco, CA 94012

Carmen Chu, City Administrator
Office of the City Administrator
1 Dr. Carlton B. Goodlett Place, Room 362
San Francisco, CA 94012

Dear President Mandelman, Members, and City Administrator Chu:

The Office of the Controller (Controller), City Services Auditor (CSA), Audits Division, presents its report on the audit of the Acquisition of Surveillance Technology Ordinance of the City and County of San Francisco (City). The audit had as its objectives to determine whether the Committee on Information Technology (COIT) and city departments have complied with the requirements of the law, which passed in 2019.

The audit concluded that, while COIT and departments have made progress in implementing it, the law does not enable the City to use a risk-based approach to match the level of oversight for different proposed uses of surveillance technology to the risks they pose. As a result, the City may be wasting resources by closely monitoring low-risk uses.

The report makes six recommendations—one to the Board of Supervisors and five to the Office of the City Administrator, which oversees COIT—to improve the City's framework for overseeing surveillance technology. Key recommendations include amending the ordinance to remove barriers to changing the process as needed and exploring a risk-based model. The responses of the Board of Supervisor and Office of the City Administrator are attached as appendices. CSA will work with the auditees to follow up every six months on the status of the open recommendations made in this report.

CSA appreciates the assistance and cooperation of all staff involved in this audit. For questions about the report, please contact me at mark.p.delarosa@sfgov.org or 415-554-7574 or CSA at 415-554-7469.

Respectfully,

Mark de la Rosa
Director of Audits

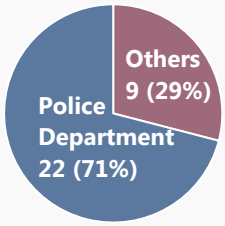
cc: Board of Supervisors
Budget Analyst
Citizens Audit Review Board
City Attorney
Civil Grand Jury
Mayor
Public Library

Executive Summary

The City and County of San Francisco (City) Acquisition of Surveillance Technology Ordinance aims to protect privacy and civil liberties. The law requires the City to disclose such technology and report on its use yearly. The Committee on Information Technology (COIT) helps to guide and advise departments in meeting the law's requirements.

Why It Matters

The Acquisition of Surveillance Technology law aims to protect residents' privacy rights and safeguard their personal data. The City must make some changes to ensure the law, and its implementation, do just that.

WE RECOMMEND	WE FOUND
Improve the surveillance technology law to allow the City to adjust the level of oversight to match the level of risk. Finding 1	The law requires the same approval process for every use of surveillance technology, regardless of its risk to privacy. In contrast, the City of San Jose assesses privacy risks and increases the level of outreach, review, and monitoring as the risks increase. Risk: Low → Mid → High **San Jose Oversight Elements** None + Use plan + Public comment window + Annual monitoring + In-person outreach + City Manager's Office review + City Council review
Designate an oversight entity and ensure it has the authority and resources to adequately oversee surveillance technology. Finding 2	With no entity assigned to monitor compliance with the law, **the City has delays and gaps in oversight** of surveillance technology use, including: ▪ **Delays in public disclosure** of privacy risks from exigent use ▪ **Conflicts of interest**, costly **legal risks**, and an inability to identify trends in addressing complaints alleging violations of the law ▪ **Limits to transparency** with delayed reporting
Increase compliance with the surveillance technology law. Findings 3 & 4	The City still **does not have use policies** for 31 pre-existing technologies.  **Positive Progress** As of August 2024 the City had established 53 use policies for technologies.

Contents

List of Exhibits

Glossary

Admin Code	San Francisco Administrative Code
Annual report	Annual Surveillance Report – The yearly summary departments must submit describing the effectiveness of the technology and the privacy impact of its use (San Francisco Administrative Code, Section 19B.6). A December 2024 amendment to the law changed this requirement to biannual.
Board	Board of Supervisors
City	City and County of San Francisco
City Administrator	Office of the City Administrator
City Attorney	Office of the City Attorney
COIT	Committee on Information Technology, which is overseen by the Office of the City Administrator
Controller	Office of the Controller
CSA	City Services Auditor, Audits Division
District Attorney	Office of the District Attorney
Impact report	Surveillance Impact Report: A review of what impact a department's use of a technology could have on the community, including what information will be gathered and how the data will be used.
Ordinance (or "the law")	Acquisition of Surveillance Technology Ordinance (San Francisco Administrative Code, Chapter 19B)
Police	Police Department
Sheriff	Sheriff's Department
Surveillance technology	Device, software, or system designed or primarily intended to collect, retain, process, or share data associated with an individual or group. (San Francisco Administrative Code, Section 19B.1)
Urgent use	Use of surveillance technology under the ordinance's exigent circumstances provision, which defines this as the immediate use of surveillance technology or the information it provides when required by an emergency involving imminent danger of death or serious physical injury to any person. (San Francisco Administrative Code, Sections 19B.1 and 19B.7)
Use policy	Surveillance Technology Policy: A document using information from the impact report to define how a department will collect and use data with that technology.

Key terms used in the report.

Introduction

BACKGROUND

The Acquisition of Surveillance Technology Ordinance[1] (the ordinance or law) aims to ensure the responsible use of surveillance technology as well as associated data, and the protection of City and County of San Francisco (City) residents' civil rights and liberties. It became law in June 2019 as part of the San Francisco Administrative Code (Admin Code). To fulfill its goals, the ordinance requires city departments to disclose surveillance technologies and report on their use annually. Also, departments must get the Board of Supervisors (Board) to approve a surveillance technology use policy (use policy) for any existing technology they use before they can purchase new surveillance technology or use data from a technology owned by other entities. The Committee on Information Technology (COIT) helps to guide and advise departments in meeting the law's requirements.

Ordinance Timeline

June 2019	Ordinance approved
August 2019	Inventory of all city uses of surveillance technology due
July 2021	Board adopts first use policy
March 2024	Voters approve new exemptions to law for Police Department
December 2024	Board passes amendment for procedural changes for COIT and reducing reporting requirements.

Surveillance Technology and San Francisco's Oversight Law

The ordinance defines surveillance technology as:

> *"any software, electronic device, system utilizing an electronic device . . . designed, or primarily intended to collect, retain, process, or share audio, electronic, visual, location, thermal, biometric, olfactory or similar information specifically associated with, or capable of being associated with, any individual or group."*

The law exempts 17 types of technologies, including emergency dispatch and communication systems. Because they are county functions,[2] the District Attorney's Office (District Attorney) and Sheriff's Department (Sheriff) are exempted from complying with the law when it would obstruct investigative or prosecutorial functions. Beyond these exemptions, the law allows temporary use of technologies without board-approved use plans in exigent circumstances (urgent use).

[1] Ordinance 107-19 created San Francisco Administrative Code Chapter 19B.
[2] California Constitution Article XI establishes the City's authority to make local laws, but they must not conflict with state laws, including one establishing *counties'* authority to make local law and requires a sheriff and district attorney as county officers.

Proposition E of 2024

Approved by San Francisco voters in March 2024, Proposition E made several changes to requirements for the Police Department (Police). It exempts the Police Department's use of drones for vehicle pursuits that could include facial recognition technology. It also exempts public safety cameras[3] used by the Police from the requirements of 19B. It allows new uses of surveillance technology without a use policy for up to a year before Police must submit a proposed policy to the Board. Furthermore, the department can continue to use the surveillance technology as long as it takes to get the use policy approved by the Board.

Committee on Information Technology

COIT is the City's governing body for technology, advising the Mayor's Office and Board, and guides the City's technology use policy. COIT provides a forum for city leadership to coordinate and collaborate to make citywide technology decisions and is overseen by the Office of the City Administrator (City Administrator). In response to the ordinance, COIT established the Privacy and Surveillance Advisory Board,[4] a body of subject matter experts, to review all ordinance requirements and provide recommendations to COIT. Exhibit 1 summarizes the law's requirements.

Impact Reports and Use Policies

Before initiating a procurement for information technology, departments must certify to the Office of Contract Administration that they have completed COIT's (Admin Code) Chapter 19B Surveillance Technology Applicability and Exemption test. This test requires departments to answer a series of questions that determine whether the item they want to buy is considered surveillance technology and if there is a board-approved use policy that covers the proposed use of the surveillance technology. According to COIT, if a department's proposed purchase is subject to the ordinance and needs an approved use policy, COIT staff contacts the department with instructions to complete a Surveillance Technology Toolkit, which collects information digitally to automatically generate a draft impact report and a draft use policy.

[3] The Admin Code, Chapter 19, defines a public safety camera as "any digital recording surveillance system installed at fixed locations in an open and obvious manner by the City and County of San Francisco to film public streets, sidewalks or common areas of public housing complexes for the purpose of enhancing public safety."

[4] The advisory board's current members are employees of the Department of Technology, Airport Commission, Digital Services, DataSF (the City's Open Data website), Office of the City Administrator, and Office of the Controller.

Exhibit 1: City law sets requirements for surveillance technology use, transparency, and monitoring.

New Acquisitions of Surveillance Technologies		
1. Departments	Submit a surveillance impact report (impact report) to Committee on Information Technology (COIT) outlining how they will use the surveillance technology and data.	
2. COIT	Use impact report to develop[a] a surveillance technology policy (use policy) and recommend that Board adopt, adopt with modification, or decline to adopt use policy.	
3. COIT & Departments	Post on their websites impact report and proposed policy 30+ days before Board meets to consider each technology.	
4. Board	If it finds benefits of using the technology outweigh its costs and use policy will safeguard civil liberties and civil rights, Board will adopt use policy into law.	
5. Departments	Post use policy on their websites within 10 days of Board approval.	
Annual Requirements		
Departments	Submit an Annual Surveillance Report (annual report) to Board and COIT by November 1st and make all annual reports available online.[a]	
Controller	Annually audit use of surveillance technology by departments.	
Existing Surveillance Technologies		
Departments	Submit an inventory of all surveillance technology by August 29, 2019.	✓ COIT collected and reviewed inventories from departments.
COIT	Publish complete inventory online.	✓ Completed.
Departments	Submit a proposed use policy for each surveillance technology to Board by December 27, 2019.[b]	✗ Incomplete (see Finding 3).

Exigent Circumstances	**Allegations of Violations**
Departments can use surveillance technology without an approved use policy during exigent circumstances and must submit a report summarizing such use to Board.	Departments must post on their websites corrective actions taken to address any complaint. Anyone impacted by a department's substantiated violation of the law can take legal action against the City after providing the allegation(s) in writing and allowing the City 30 days to correct the problem.

Notes:

[a] A December 2024 amendment to the law modified COIT's role and changed reporting from annual to biannual.

[b] COIT states the number of policies, need for review by the Office of the City Attorney (City Attorney), and staffing limitations made this date unachievable. COIT granted a 90-day extension but stated it did not formally grant more extensions because it had limited resources and focused on helping departments move policies through the full legislative process.

Source: Admin Code, Chapters 19B and 2A

Monitoring Reports

During the period covered by this audit, for each surveillance technology a department uses, it was required to submit an annual report by November 1st describing how the technology was used, whether it was effective, what data was collected, and other information to demonstrate whether the benefits of using the technology outweighed the financial cost and privacy risks. The City amended the law in December 2024 to change the reporting requirement to every two years instead of every year.

2024 Procedural Changes in the Ordinance

After the audit period, in December 2024, the Board amended the ordinance, changing certain procedural requirements. Among other things, the ordinance no longer requires COIT to receive departments' impact reports and develop a use policy. The amendment also changed the requirement for departments to submit monitoring reports from an annual report for each technology to a combined report for all the department's technologies every two years.

Why It Matters

San Francisco passed a surveillance technology law to safeguard civil liberties and civil rights. The City must make sure the law, and its implementation, do just that.

OBJECTIVE

The objective of this audit was to determine whether COIT and city departments complied with the requirements of the Admin Code, Chapter 19B. The law requires the Office of the Controller (Controller) to conduct annual audits.[5]

SCOPE AND METHODOLOGY

The audit scope covered the compliance of city departments and COIT with the Admin Code, Chapter 19B. For annual monitoring provisions, the audit scope covered calendar year 2022 and 2023 reports. For impact report and use policy provisions, the audit scope covered use policies approved before November 9, 2023, when CSA established the audit's final scope and objectives.

To achieve the objective, we:

- Reviewed requirements of the ordinance, recent changes to it, and related guidance for departments' compliance.

[5] Admin Code, Section 2A.20(d)(2).

- Tested compliance with procedures to acquire or use surveillance technology using a convenience sample of 11 of 22 departments with board-approved use policies. We tested one technology from each department.
- Tested compliance with annual monitoring using a separate convenience sample of 12 departments with use policies approved by the Board in 2021, and therefore subject to annual reporting requirements in 2022 and 2023. We tested one technology from each department.
- Reviewed similar laws or policies and interviewed representatives of the City of Portland (Oregon), City of San Jose, and County of Santa Clara on the implementation of their law or policy.
- Reviewed relevant past audits of the City and County of San Francisco, audits from the City of Dallas (Texas), City of Seattle (Washington), and State of California, and relevant media coverage and court cases.
- Interviewed key personnel of COIT, the City Attorney, and city departments for the technologies in our samples.

Results

Finding 1 – Vulnerabilities in San Francisco's surveillance technology ordinance risk privacy abuses, but a risk-based approach could strengthen oversight and more efficiently use city resources.

The ordinance creates inconsistent oversight of some technologies, such as body-worn cameras and facial recognition software, exempts some technologies not based on the degree of risk they pose but on which department owns them, and treats all the remaining technologies the same regardless of the impact on privacy they may have. The law is also administratively burdensome, as found in a previous audit.

Broad and Inconsistent Exemptions for Criminal Justice Departments

The ordinance exempts or loosens oversight for many technologies used by the City's criminal justice system.

District Attorney and Sheriff Exemptions

In California, the district attorney and sheriff are county functions, and state law bans cities from making laws that would interfere with their ability to prosecute or investigate crime. Rather than complying with the ordinance like other departments, the District Attorney and Sheriff only need to explain how compliance will obstruct their prosecutorial or investigative functions in a letter to the Controller and the Clerk of the Board.

We found that the District Attorney has 26 and the Sheriff has 22 surveillance technologies that are exempt from oversight under the ordinance. The certification letters that resulted in these exemptions state that the information the impact reports and use policies require the departments to disclose would give criminals insight into the investigative processes that might help them avoid detection. In March 2024 voters approved additional exemptions that apply to Police. Exhibit 2 shows the differences in how the ordinance applies to the City's criminal justice departments.

Exhibit 2: Whether the surveillance technology ordinance applies and how the City applies it depends on which criminal justice department uses the technology

For instance, GPS location tracking used by the Sheriff is entirely exempt but must comply with the law when used by the Police Department, Adult Probation Department, or Juvenile Probation Department.

Department	Exemption	Differences in Application	Examples of Technologies
District Attorney	**Broadly exempt**	Exemption based on self-certification that applying the ordinance would impede investigative or prosecutorial functions	• Facial recognition software • GPS location tracking • Web-scraping tools
Sheriff	**Broadly exempt**	Exemption based on self-certification that applying the ordinance would impede investigative or prosecutorial functions	• Body-worn cameras • Drones • Facial recognition software • GPS location tracking • Wearable alcohol monitors
Police	**Partial exemption**	*Exempt*: Body-worn cameras; public safety cameras;* aerial drones for vehicle pursuits, which may use facial recognition technology Can pilot new technology uses for a year before presenting a use policy to the Board for approval.	• Body-worn cameras • Fixed surveillance cameras • GPS location tracking • Drones, including those that use facial recognition, for vehicle pursuits • Web-scraping tools
Adult Probation Juvenile Probation	Not exempt	None	• Wearable alcohol monitors • GPS location tracking
Police Accountability	Not exempt	None	Social media monitoring
Public Defender	Not exempt	None	None

* A public safety camera is a digital recording surveillance system installed at fixed locations in an open and obvious manner by the City to film public streets, sidewalks, or common areas of public housing for the purpose of public safety.

Source: Analysis of Admin Code, Chapters 19B and 96I; COIT's inventory of surveillance technology; exemption letters

Police Department Exemptions

With San Francisco voters' passage of Proposition E in March 2024, the Police Department is now partially exempt from the ordinance. Specifically, the department no longer needs to get board-approved use policies to:

- Use **aerial drones** for vehicle pursuits, including use of facial recognition software on the drone's video.
- Use body-worn cameras.
- Install public **surveillance cameras**. (This now only requires the authorization of the chief of police.)
- **Pilot technology for up to one year** without a use policy and can continue using the technology until the Board approves or denies the policy submitted after the one-year pilot period.

The intent of these partial exemptions is to remove some of the administrative burden, so the Police Department can more efficiently use such technologies and improve its effectiveness.

Risk Created by Exemptions

To allow criminal justice departments to be fully or partially exempt from the City's surveillance technology oversight process undermines the law's intended civil liberty protections. It increases the risk of abuses, such as monitoring individuals inappropriately or profiling groups based on race, religion, or another protected status. It allows city departments to track data on members of the public without a use policy that balances operational needs with adequate safeguards for civil rights, and the public comment period, COIT oversight, and Board's approval that come with it.

These exemptions may also expose the City to legal risk. Exhibit 3 summarizes some court cases centered on questions about whether using certain forms of surveillance technology violated civil rights.

Exhibit 3: Use of surveillance technologies is at the center of some civil rights court cases

Case	Alleged Misuse of Surveillance Technology	Outcome
United States v. Jones (2012)	In a narcotics investigation, the FBI installed a GPS tracker on a car the subject drove.	The extended tracking of 28 days was ruled an **unreasonable search** and was the basis for reversing Jones' conviction. Determining the legality of the GPS tracking took four years.
United States v. Tuggle (2021)	Federal agents watched a suspect's home for 18 months using cameras they installed on nearby utility poles without a warrant. The cameras recorded nearly 100 suspected meth deliveries at the suspect's house, and the pole camera footage helped indict him on two drug charges.	The court ruled the actions permissible, but the department's use of the surveillance technology is **described in the ruling as "concerning" and expressed "unease" about the implications for future surveillance.**
FBI v. Fazaga (2022)	The FBI allegedly used a paid informant to covertly record activities at mosques, where they indiscriminately gathered hundreds of worshippers' names, phone numbers, email addresses, and information on their religious and political beliefs, violating their constitutional right to religious freedom.	**Case dismissed** based on the state secrets privilege defense, which excludes evidence when the government asserts court proceedings might disclose sensitive information and endanger national security. The case took 11 years.

Source: Harvard Law Review: "United States v. Jones." Volume 126, no. 1 (2012); "Fazaga v. FBI." Volume 133, no. 5 (2020); "United States v. Tuggle." Volume 135, no. 3 (2022)

Use of City Resources Should Be Strategic

The City has limited capacity to handle privacy matters, but the ordinance requires COIT to spread its attention equally across all surveillance technologies, regardless of risk.

Alternative to Exemption

The ordinance's exemptions for criminal justice departments weaken oversight of how they use surveillance technologies and increase the risk of the technologies being abused. Other than those subject to exemptions, all surveillance technologies in the City go through the same approval process, regardless of risk. For example, a people counter, a device that anonymously counts people as they enter a park, is subjected to the same process as an aerial drone with facial recognition capabilities.[6] The City may be wasting resources by applying a high degree of oversight on low-risk uses, while exempting high-risk uses from any oversight.

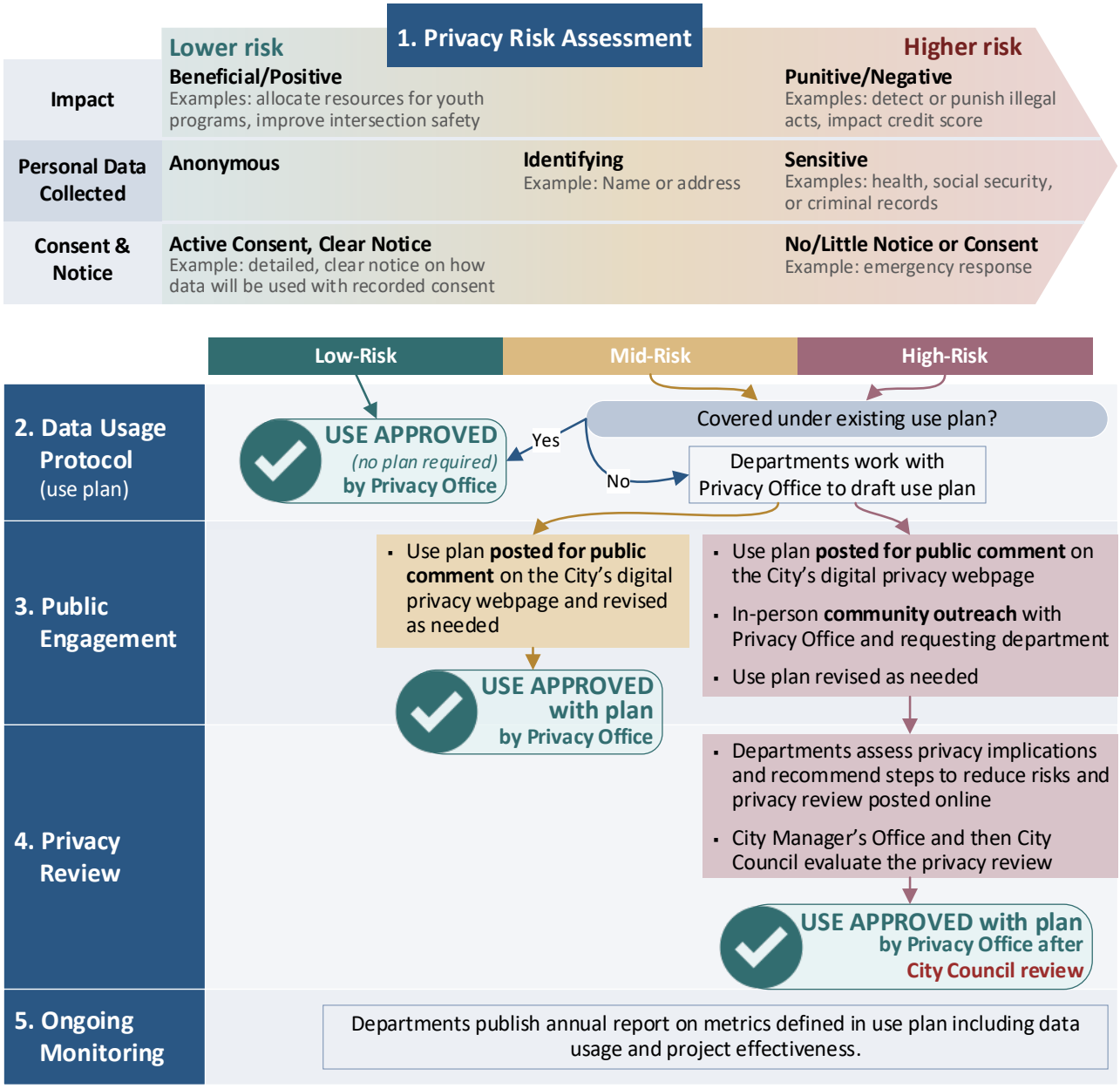
The City can explore other options. Rather than exempting technologies for criminal justice departments, the City could modify the process to keep sensitive information confidential while still requiring use plans and monitoring reports. Also, the City could remodel its oversight program to apply a risk-based approach that could better match the degree to which a technology is monitored to the risk associated with its use rather than the level of oversight being dictated based on which department is using it. However, changing the process would require amending the law to remove barriers that prevent the City from changing the process for law enforcement, such as exempting certain information from public disclosure.

A Risk-Based Approach to Data Privacy Protection

San Jose's Digital Privacy Office assesses the risk of a proposed use of technology based on intended impact, type of data collected, and notice or consent provided. This risk assessment determines whether the technology's use requires additional review, a Data Usage Protocol (use plan), and/or public engagement. Low-risk uses can usually be approved with minimal review. Mid-risk uses may require additional live discussions and may be published for public comment. High-risk uses require a public comment period and a more thorough privacy review and discussion with the requesting department. San Jose's Digital Privacy Office may approve or reject the technology's use or require adjustments to the Data Usage Protocol before approval. Adjustments may require shifts in what data can be collected, how it can be collected, and how it can be used. Exhibit 4 shows how San Jose's privacy review process varies based on how its Privacy Office categorized the technology use's risk.

[6] The ordinance prohibts the use of facial recognition technology, but not the purchase of technologies that have facial recognition capabilities as long as they do not use the facial recognition function.

Exhibit 4: San Jose bases its approval of surveillance technology on risk, requiring City Council approval only for high-risk uses



Source: CSA generated from City of San Jose Digital Privacy Handbook and interview of San Jose's Privacy Office staff

According to COIT, it did not receive additional funding to implement the ordinance, so had to repurpose existing resources by assigning one full-time employee to administer the ordinance. In comparison, San Jose had four full-time employees and one part-time employee in its Privacy and Artificial Intelligence team according to San Jose's privacy officer. If it applied a risk-based model as San Jose does, the City could streamline approvals and focus its resources on oversight for higher-risk technologies.

Finding 2 – The City has not established clear authority or responsibility for oversight of surveillance technology.

The City lacks a single entity to oversee departments' compliance with multiple components of the ordinance, preventing the City from fully understanding whether departments are appropriately using surveillance technology and informing the public and policymakers as required. Furthermore, the City may expose itself to legal risks without greater oversight. As discussed in the Introduction, the ordinance includes multiple reporting and posting requirements for city departments that use surveillance technology, including its use during urgent circumstances. However, there is no single entity in the City that monitors departments' compliance with these sections of the ordinance, as described in Exhibit 5.

Exhibit 5: The City lacks an entity assigned to monitor departments' compliance with some sections of the ordinance, leading to oversight gaps and delays

Although the law tasks COIT with administrative duties, it does not empower COIT with authority or responsibility to monitor compliance with the law's requirements regarding urgent use, addressing complaints, or transparency.

Urgent Use	Complaints	Transparency
Using technologies without an established use policy is allowed in "exigent circumstances." However, transparency of such uses relies on departments' self-reporting, and those reports are not due until 60 days after use.	Departments disclose complaints of ordinance violations in monitoring reports, including their self-reported corrective measures. If departments do not self-report this information, there is no way for the Board, COIT, or the public to know about complaints.	Departments must post on their websites their use policies, monitoring reports, and a description of how they addressed complaints. However, there is: • no monitoring of compliance with posting requirements. • no requirement to post exigent use reports.
Why This Matters		
• City cannot quickly identify if use of surveillance technology under exigent circumstances **is appropriate**. • Public does not have **timely transparency** into privacy risks associated with urgent use.	• **Conflicts of interest** may result from departments investigating allegations against them with no oversight. • **Costly legal risk** if City fails to fix violations within 30 days of written notice. Ordinance allows those affected to take legal action and requires City to pay their court costs.	• **No transparency** about urgent use and complaints, if departments fail to post information online. • **Limited transparency** of impact reports, use policies, and monitoring reports due to inconsistent compliance.

Source: CSA analysis of Admin Code, Chapter 19B (sections 7 for urgent use, 6 and 8 for complaints, and 3, 6, and 7 for transparency); interviews of COIT staff

The City may never become aware of departments' noncompliance in some cases, but we identified some instances.

Although the ordinance allows departments to use surveillance technology without an approved use policy in urgent circumstances, they must end use within 7 days and submit a written report summarizing use to the Board within 60 days.[7] The Police Department submitted four of six such reports on time, but submitted two late - one by 8 days and the other by 45 days.[8] The department stated it submitted the first report late because it was the department's first such report and staff spent additional time to ensure it followed the process correctly. The department stated it submitted the second report late because staff were unclear about whether the specific incident was covered by the ordinance's requirements.

Although these causes are reasonable, the delays reinforce the importance of having a single entity to monitor departments' use of surveillance technology during urgent circumstances and ensure the public and key decision-makers are kept informed and can respond to any needed policy change that may be raised by such use.

Finding 3 describes an example where a complaint turned into legal action, and Finding 4 concerns instances in which departments did not post required information online, or did so late, both decreasing transparency and depriving stakeholders of the opportunity to comment on use policies before they become law.

In contrast, the City of San Jose exerts stronger oversight. According to its privacy manual, the San Jose Digital Privacy Office requires departments to submit performance metrics as part of San Jose's Annual Data Usage report (see comparison of metrics to San Francisco's annual reporting in Finding 4). Also, in San Jose's 2023 annual reports on the use of a gunshot detection system and automated license plate readers, the Digital Privacy Office reported that it had reviewed access logs, system accuracy, and program summaries to verify that the San Jose Police Department complied with its use plans.

Under San Francisco's ordinance[9], the City Administrator or its designee is authorized to adopt standards that guide departments in implementing the ordinance, after notice and a public hearing. This positions the City Administrator (or its designee) as the agency best able to monitor and oversee citywide compliance with the ordinance.

[7] Admin Code, Section 19B.7.
[8] Because no central tracking of exigent use exists, we only reviewed exigent use reports posted on departments' websites. We found that only the Police Department has posted any such reports. We did not determine whether other departments had exigent uses.
[9] Admin Code, Section 19B.9.

COIT reports that it works with departments to help create use policies and subsequently help them move policies through the full legislative process which supports the guidance role the law provides for it. As explained in Finding 1, COIT may not have sufficient resources or authority to adequately monitor departments and enforce the ordinance.

Finding 3 – Years after the ordinance's passage, 31 surveillance technologies that existed before the ordinance still do not have a board-approved use policy.

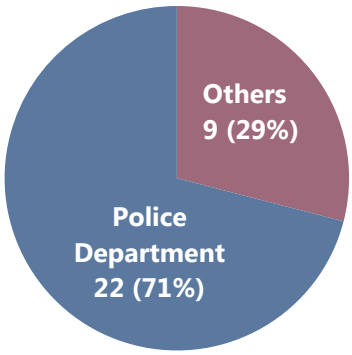
Positive Progress

The City had established 53 use policies for surveillance technologies as of August 2024.

The City has been using 31 surveillance technologies for over five years (since the ordinance passed) without the input or approval from the public or policymakers that comes from establishing a board-approved use plan and impact import. Therefore, the City is less able to ensure that surveillance technology is used in ways that adequately safeguard civil liberties and rights.

The ordinance calls for departments using surveillance technology before the ordinance passed to submit an impact report and proposed use policy to the Board. However, the ordinance allows departments to continue using pre-existing surveillance technology without an approved policy until the Board approves or denies a proposed use policy.

Exhibit 6: The Police Department owns 22 of 31 pre-existing surveillance technologies that lack a board-approved use policy



Source: CSA analysis of COIT inventories

Of the 31 pre-existing technologies without a board-approved policy, most belong to the Police Department, as shown in Exhibit 6. The department has approved policies for some technologies, including automated license plate readers, ShotSpotter,[10] and surveillance cameras. However, 22 technologies, including GPS tracking devices and reconnaissance robots used for special police operations, are still without policies. This situation potentially exposes the City to legal risks and expenses. For example, in June 2023 the Police Department received a letter from Secure Justice[9] alleging the department had violated the ordinance because it did not submit the required use policies and impact reports to the Board on time. The law gives the City 30 days after receiving such a written notice to remedy the violation. As noted in Finding 2, the law allows anyone affected by an alleged violation to take legal action against the City if it does not meet the 30-day deadline. In July 2024 Secure Justice initiated legal action against the City in this matter.

According to COIT, not all pre-existing technologies have an approved use policy within the required period due to limited staffing

[10] ShotSpotter is a gunshot detection system that records sounds and uses sensors to locate the origin of the shots.

at COIT and varied capacities at departments. In addition, COIT stated that the impact of the COVID-19 pandemic on city workers and operations caused further delays.

Finding 4 – Some departments did not fully comply with the ordinance, but some of the ordinance's requirements duplicate the legislative process.

Some departments did not adequately comply with all requirements of the law. During the approval process, most departments did not comply with procedures specified in the ordinance, but this noncompliance does not have a significant impact because the requirements largely duplicate the legislative process. The annual reporting requirement is meant to give stakeholders information that allows them to assess whether the benefits of using the surveillance technology are worth the cost and the risks to the public's privacy. However, poor quality reports do not provide this information.

The ordinance requires departments to take steps to give the public access to proposed use policies and to get them reviewed by other city stakeholders. Specifically, it requires departments to first approve and then submit proposed use policies to the City Attorney and Mayoral Offices for review before the Board considers them.[11] It also requires departments to post use policies, impact reports, and annual reports on their departmental websites at certain points in the process. However, these requirements are largely duplicative of the legislative process, as shown in Exhibit 7.

[11] The December 2024 ordinance amendment removed this requirement.

Exhibit 7: Some requirements of the surveillance technology ordinance duplicate and are out of sync with San Francisco's legislative process

Some departments do not comply with some of these requirements, but the noncompliance does not interfere with transparency or oversight because the legislative process already provides it.

Surveillance Technology Approval Process Requirements Stated in Ordinance[a]	Legislative Process for Enacting City Ordinances
1. **Department** approves internally.	1. **City Attorney** approves draft ordinance.
2. Submit to **city attorney** for review and to the **Mayor**.	2. **Department head or commission** introduces at a **Board** meeting. Use plan as draft ordinance **posted** to Board's website.
3. Submit to the **Board of Supervisors (Board)**.	3. Standing committee of the Board reviews proposed ordinance and makes a recommendation.
4. **Post**[b] on department website proposed use policies and impact reports **30 days** before being heard by the Board.	4. Board approves at a meeting of the full Board that must be at least **30 days** after meeting when proposed use policy was introduced.
5. **Post**[b] **final use policies** on department website within ten days of Board approval.	5. Board approves again at a second meeting of the full Board Approved ordinance **posted**[b] to Board's website.
	6. **Mayor** approves or vetoes ordinance.

Notes:
[a] December 2024 ordinance amendment eliminated some duplicative and illogically ordered steps, such as step 2.
[b] Ordinance requires posting to departments' websites, while legislative process is posted on Board's website.

Source: San Francisco Charter, Chapter 19B, for ordinance requirements; Board of Supervisors 2022 Legislative Handbook for legislative process for ordinances

Some annual reports are of poor quality

They do not adequately describe how effective the technology is or how well the department safeguards people's privacy.

Poor-quality annual reports

Once the City has use policies, the annual monitoring reports departments must submit are intended to allow stakeholders to confirm that the benefits to the City from using the technology outweigh the risks to the public's privacy. Although departments submitted these reports on time for all 12 technologies we reviewed, the poor quality of the contents of some of these reports do not allow stakeholders to assess the technologies' costs and benefits.

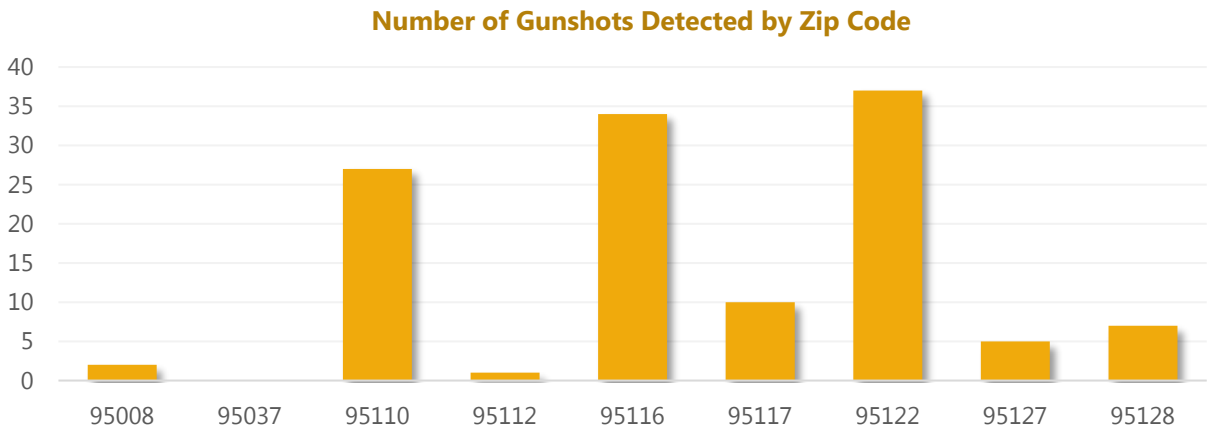
Annual reports should present the data that was collected and information to help the Board assess the effectiveness of the technology in achieving the intended goal. However, some reports simply do not do so. For example, the Fire Department's annual report on drone use states only that "The technology has been used

according to policy," with no details on what it was used for or how. In another example, the Department of Homelessness and Supportive Housing's annual report on use of security cameras states, "our security camera has been effective in providing security for the safety of our shelter clients" with no further explanation or supporting data. Such weak annual reporting does not assure stakeholders that the City's money was well spent on the surveillance technology or that any reported improvement to city operations is worth the risks to the public's privacy.

In contrast to San Francisco's reports, San Jose's annual reports analyze both the effectiveness of the technologies and privacy concerns, as discussed in Finding 2. As shown in Exhibit 8, San Jose's annual data usage reports provide detailed metrics on the effectiveness of the city's gunshot detection technology. The example shows how accurate the technology is in detecting gunshots, which could help decision-makers assess its benefit. Meanwhile, the most recent equivalent report in San Francisco, which is produced by the Police Department, includes only how many alerts the system triggered, with no analysis of its accuracy.

Exhibit 8: San Jose's annual monitoring requires departments to submit performance metrics and analyses to support the effectiveness of their surveillance technology

Date	False Positives	False Negatives	True Positives	Duplicative Positives	Unknown
2/25-7/7	42	N/A	61	6	20
7/8-12/31	9	N/A	111	4	17
Total	**51 (19%)**	**N/A**	**172 (64%)**	**10 (4%)**	**37 (14%)**



Source: City of San Jose's Annual Data Usage Report for Gunshot Detection Technology, January–December 2023

RECOMMENDATIONS

The Board of Supervisors should:

1. Amend the surveillance technology ordinance to remove barriers so the Office of the City Administrator can implement a risk-based approach to administering the ordinance. The goal should be to make the oversight procedures commensurate with the level of risk each technology poses to privacy.

The Office of the City Administrator should:

2. As authorized in the San Francisco Administrative Code, Section 19B.9, formally designate an entity that can adopt operational standards and interpretive guidelines to assist and guide departments in implementing the surveillance technology ordinance.

3. Ensure the designated entity has adequate resources, including the option of temporary positions, to effectively monitor compliance with the ordinance, coordinate with departments, and address the backlog of pre-existing technologies that currently lack approved use policies.

4. Ensure the designated entity establishes and issues rules, operational standards, and interpretive guidelines that will help departments comply with the surveillance technology ordinance. The guidance should address how to communicate changes to the law, policy, or procedures, and set expectations for departments' compliance with reporting requirements.

5. Ensure the designated entity encourages departments to provide information in their annual reports that demonstrates whether the benefits of using the technology are worth the financial cost and risk to the public's privacy.

6. Analyze alternative ways to administer oversight of surveillance technology and present its findings to the Board of Supervisors. The analysis should include approaches that apply a risk framework to tailor the scope of oversight activities to the privacy risks of the proposed technology use and approaches to monitoring criminal justice departments that balance department operational needs, oversight, and confidentiality of sensitive systems and processes.

Appendix | Department Responses

Board of Supervisors

President, Board of Supervisors
District 8

City and County of San Francisco

RAFAEL MANDELMAN

September 15th, 2025

Mark de la Rosa
Director of Audits
Office of the Controller - City Services Auditor
1 Dr. Carlton B. Goodlett Place, Room 476
San Francisco, CA 94102

Dear Mr. De la Rosa

As instructed in your email on February 26th, 2025 titled *Draft Memorandum for Your Response: The City Needs Risk-Based Monitoring of Surveillance Tech and Better Oversight Across Criminal Justice Departments*, enclosed please find the San Francisco Board of Supervisors completed Recommendation and Response form.

If you have any questions or concerns, please contact my Legislative Aide Melanie Mathewson at melanie.mathewson@sfgov.org.

Sincerely,

Rafael Mandelman,
President, San Francisco Board of Supervisors

Committee on Information Technology

City & County of San Francisco
Daniel Lurie, Mayor

Office of the City Administrator
Carmen Chu, City Administrator
Edward McCaffrey, Director
Committee on Information Technology

Thursday, July 31, 2025

Mark de la Rosa
Director of Audits
Office of the Controller, City Services Auditor
City Hall, 1 Carlton B. Goodlett Place, Room 316
San Francisco, CA 94102

Re: Response to the 2025 COIT Surveillance Technology Audit Report

Dear Mr. de la Rosa,

The Office of the City Administrator has received and reviewed the draft report titled, "The City should consider risk-based monitoring of surveillance technology" from the City Services Auditor. The City Administrator and staff from the Committee on Information Technology (COIT) appreciate the time and effort spent on compiling this report and thank you and your team for providing us with an opportunity to assess and respond. As the department that oversees the City's data privacy and surveillance technology program, we appreciate the recognition from the Office of the Controller that COIT is in compliance with the requirements of Chapter 19B of the Administrative Code related to surveillance technology plans, transparency, and monitoring of this critical issue.

Since Chapter 19B became effective in June 2019, COIT has collaborated with City departments to facilitate compliance with the law resulting in approval of over 200 surveillance technologies for use in the City and County of San Francisco. COIT maintains an up-to-date and transparent online inventory, which is accessible to the public, posts the most current version of Surveillance Technology Policies (STP) and any subsequent amendments, and has implemented a process for the Annual Surveillance Report. Over the last six years, COIT has cultivated a collaborative relationship with over 30 departments through active outreach and privacy education to create policies benefitting both the public and the City. This work has resulted in 78% of the Surveillance Technology Inventory either having a Board of Supervisors (BOS) approved STP or in the process of seeking approval.

Since its adoption in 2019, COIT has worked tirelessly to implement Chapter 19B as it was conceived and intended – to protect the data privacy of all San Franciscans. COIT staff has sought to continuously improve surveillance technology management by establishing a surveillance reporting process in which learnings from the previous reporting year are integrated into the next. Additionally, in 2024, COIT supported amendments to Chapter 19B resulting in passage of legislation by the Board of Supervisors to streamline the reporting process, while maintaining privacy protections. As COIT staff continues to identify ways to strengthen protections and eliminate bureaucracy, we appreciate the Office of the Controller's partnership.

SFGSA.org · 3-1-1

Despite limited staffing, COIT has created a successful and effective program to implement Chapter 19B. COIT has developed a culture of collaboration with departments, successfully fostering acceptance and appreciation of privacy work and making the San Francisco safer.

COIT staff will continue to follow the law as established by Chapter 19B, regularly consulting with the City Attorney to ensure that staff interprets the law correctly. Additionally, COIT will continue to educate, guide and support City departments in the effort to prioritize privacy.

Again, we would like to thank you and your team for the work on this report over the last two years, and COIT will continue to prioritize the privacy of San Franciscans through our work and guidance to departments.

Sincerely,

Edward McCaffrey
Director
Committee on Information Technology

cc:
Carmen Chu, City Administrator, Office of the City Administrator
Katharine Petrucione, Deputy City Administrator, Office of the City Administrator
Julia Chrusciel, Committee on Information Technology

Recommendations and Responses

For each recommendation, the responsible agency should indicate in the column labeled Agency Response whether it concurs, does not concur, or partially concurs and provide a brief explanation. If it concurFs with the recommendation, it should indicate the expected implementation date and implementation plan. If the responsible agency does not concur or partially concurs, it should provide an explanation and an alternate plan of action to address the identified issue.

Recommendation	Agency Response	CSA Use Only Status Determination*
The Board of Supervisors should:		
1. Amend the surveillance technology ordinance to remove barriers so the Office of the City Administrator can implement a risk-based approach to administering the ordinance. The goal should be to make the oversight procedures commensurate with the level of risk each technology poses to privacy.	☐ Concur ☒ Do Not Concur ☐ Partially Concur The Board of Supervisors does not concur with this recommendation. While we recognize that a risk-based tiering system can promote efficiency by differentiating between high- and low-risk technologies, COIT has noted that the ordinance was reviewed and updated after the passage of Proposition E in Spring of 2024, and COIT has already adopted a risk-based approach in practice. Currently, all surveillance technologies are treated as having risk in order to promote equity and consistency across departments.[a]	☐ Open ☐ Closed ☒ Contested

[a] Auditor Comment to Agency Response: The changes to the legislation made in December 2024 were not in effect during the audit's scope and CSA will re-assess this issue in a future audit that will be able to take into account the changes made to the law.

* Status Determination based on audit team's review of the agency's response and proposed corrective action.

Recommendation	Agency Response	CSA Use Only Status Determination*
The Office of the City Administrator should:		
2. As authorized in the San Francisco Administrative Code, Section 19B.9, formally designate an entity that can adopt operational standards and interpretive guidelines to assist and guide departments in implementing the surveillance technology ordinance.	☒ Concur ☐ Do Not Concur ☐ Partially Concur In September 2025, the City Administrator designated COIT in writing as the entity that can adopt operational standards and interpretive guidelines to assist and guide departments in implementing the surveillance technology ordinance.	☐ Open ☒ Closed ☐ Contested
3. Ensure the designed entity has adequate resources, including the option of temporary positions, to effectively monitor compliance with the ordinance, coordinate with departments, and address the backlog of pre-existing technologies that currently lack approved use policies.	☒ Concur ☐ Do Not Concur ☐ Partially Concur By June 1, 2026, the City Administrator will determine if COIT has adequate resources to manage administration of Chapter 19B and will seek resources in the Fiscal Year 2026-27 budget if necessary.	☒ Open ☐ Closed ☐ Contested
4. Ensure the designated entity establishes and issues rules, operational standards, and interpretive guidelines that will help departments comply with the surveillance technology ordinance. The guidance should address how to communicate changes to the law, policy, or procedures, and set expectations for departments' compliance with reporting requirements.	☒ Concur ☐ Do Not Concur ☐ Partially Concur By July 1, 2026, COIT staff will publish rules, standards and/or guidelines on its website.	☒ Open ☐ Closed ☐ Contested

* Status Determination based on audit team's review of the agency's response and proposed corrective action.

Recommendation	Agency Response	CSA Use Only Status Determination*
5. Ensure the designated entity encourages departments to provide information in their annual reports that demonstrates whether the benefits of using the technology are worth the financial cost and risk to the public's privacy.	☒ Concur ☐ Do Not Concur ☐ Partially Concur By September 30, 2026, COIT staff will provide guidance to departments required to provide annual surveillance reports that they should provide sufficient information to demonstrate whether the benefits of using the technology are worth the financial cost and risk to the public's privacy.	☒ Open ☐ Closed ☐ Contested
6. Analyze alternative ways to administer oversight of surveillance technology and present its findings to the Board of Supervisors. The analysis should include approaches that apply a risk framework to tailor the scope of oversight activities to the privacy risks of the proposed technology use and approaches to monitoring criminal justice departments that balance department operational needs, oversight, and confidentiality of sensitive systems and processes.	☒ Concur ☐ Do Not Concur ☐ Partially Concur By June 1, 2026, COIT staff will undertake an analysis of methods for administering oversight of surveillance technology and present its findings to the Clerk of the Board of Supervisors via letter.	☒ Open ☐ Closed ☐ Contested

* Status Determination based on audit team's review of the agency's response and proposed corrective action.