Seattle Office of Inspector General

Consolidated Risk Surveillance Usage Review 2024

As Required by Seattle Municipal Code 14.18.060

June 6, 2025

Office of Inspector General
City of Seattle
PO Box 94764
Seattle, WA 98124-7064

206.684.3663
oig@seattle.gov

Table of Contents

Purpose

Seattle Municipal Code 14.18 governs the process through which City departments acquire surveillance technologies. Chapter 14.18.060 requires Office of Inspector General (OIG) to conduct annual reviews of the Seattle Police Department's (SPD) use of surveillance technologies, focusing on six areas:

a. Technology Use – frequency and usage patterns
b. Data Sharing – the frequency and patterns of data sharing
c. Data Security – how well SPD safeguards individual information
d. Potential Civil Liberties Impacts – real or possible impacts to civil liberties and any disproportionate impacts on disadvantaged populations
e. Internal Assessments – any internal audits, new concerns registered by community members, or complaints made to the Office of Police Accountability (OPA) about the surveillance technology
f. Annual Costs

To improve review efficiency and quality, OIG designated two levels of reporting. OIG identifies the level of review appropriate for each technology based on their risks:

- **Individual Surveillance Reviews:** New technologies or those with higher risk are evaluated through Compliance Reviews, which establish tests for compliance with internal policies, local/state laws, or a technology's Surveillance Impact Report (SIR), which is published by SPD.
- **Consolidated Surveillance Review:** Technologies that OIG has previously reviewed and carry lower risk are assessed through a survey and combined in a single report.

Methodology

Consolidated Surveillance Review Methodology

This report is a consolidated surveillance review comprising the following ten technologies:

1. Situational Awareness Cameras Without Recording
2. Remotely Operated Vehicles
3. Forward-Looking Infrared Real-Time Video Cameras
4. Camera Systems
5. Computer Cellphone and Mobile Device Extraction Tools
6. Audio Recording Devices
7. Tracking Devices
8. Automated License Plate Readers (Patrol)
9. Closed Circuit Television Cameras
10. Fusus Real-Time Crime Center Software

To inform this consolidated review, OIG conducted a risk assessment, surveyed subject matter experts at SPD, and consulted SPD internal data to provide the most up-to-date information on the capabilities, policies and procedures, and current use of each technology. Statements provided by SPD for technology in the consolidated review were not verified by OIG but were consistent with OIG's understanding of the technologies and prior findings.

Relevant Units and Their Roles

This report references various departments within SPD that use surveillance technologies. The list below includes the units who use the reviewed surveillance technologies and their role to provide additional context for the circumstances in which technologies are used:

Arson and Bomb Squad (ABS)

Investigates suspicious fires and explosions. These officers are also part of a task force with the Bureau of Alcohol, Tobacco, Firearms and Explosives, the Federal Bureau of Investigations and the Seattle Fire Department.

Harbor Unit (HBU)

Responsible for patrolling the city's lakes and waterways. These officers investigate water accidents and collisions, perform boat safety inspections, respond to boat fires, and remove debris and other hazards from the water.

Internet Crimes Against Child Unit (ICAC)

Investigates Child Sexual Exploitation (CSE) cases that might involve the production, distribution, or possession of CSE materials or where Electronic Service Provider (ESP) systems have been used for CSE crimes. CSE crimes often involve the use of computers, cellular phones, tablets or other electronic devices. Unlike other units who request approval for technologies through the Technical and Electronic Support Unit, ICAC has a separate internal approval process for some surveillance technologies due to the nature of their work.

Special Weapons and Tactics (SWAT)

Responds to incidents that include barricaded person, active shooting scenes, high risk search warrants, crowd control during large-scale disturbances or riots, sniper incidents, or terrorism threats. SWAT can also be called to support other units in high-risk scenarios.

Patrol Unit

Consists of officers who are first responders to incidents. They respond directly to service calls dispatched from the 911 center as well as proactively patrol the city's neighborhoods. When not responding directly to 911 calls, or providing backup to other officers, patrol officers use focus on ongoing crime problems in specific neighborhoods.

Technical and Electronic Support Unit (TESU)

Manages request for most surveillance technologies used by other units in the department for their investigations. TESU approves technology deployment, assists in technology deployment, extracts data, and provides data to investigating officers. To review the process of a unit acquiring a technology through TESU, see Appendix A.

Situational Awareness Cameras Without Recording

Special Weapons and Tactics (SWAT) temporarily deploys Situational Awareness Cameras Without Recording (sometimes called "pole cameras") during dangerous situations to assess safety risks to the subject of observation, the public, and officers. SWAT uses these cameras to view surroundings and gain additional information prior to entering a location. While some pole cameras have a recording option, SWAT does not retain recordings of incidents. The following is a summary of some considerations in assessing this technology:

SPD Unit	SWAT
Technology Use	SPD reported that Situational Awareness Cameras were used 42 times in 2024.
Data Sharing	Situational Awareness Cameras are not used to record. There are no data available to be shared.
Data Security	Situational Awareness Cameras are not used to record. There are no data to be safeguarded or stored.
Potential Civil Liberties Impacts	a. SWAT reports that most deployments result from a warrant, and exigent circumstances are rarely used to deploy the technology. b. Situational Awareness Cameras are used to provide additional safety in dangerous situations, and - when used according to the SIR - these cameras are not expected to impact civil liberties or have disproportionate impacts.
Internal Assessment	As of January 2025, there have been no new assessments, registered community concerns, or OPA complaints for this surveillance technology.
Costs	SWAT reported that there were no significant changes in cost to Situational Awareness Cameras in 2024. The annual cost is approximately $200.

Recommendations

As of January 2025, two recommendations related to this technology remained open:

1. SPD should amend the SIR regarding Situational Awareness Cameras Without Recording to reflect current inventory.
2. SPD should update the SIR regarding Situational Awareness Cameras Without Recording to reflect the recording functionalities of these cameras or disable these recording features via technical control.

Most recent Compliance Review: Situational Awareness Cameras Without Recording (2021 and 2022)

Remotely Operated Vehicles

Remotely Operated Vehicles (ROVs) are a class of unarmed, motorized devices used to surveil subjects and perform basic manual tasks at a safe distance. SPD owns 14 ROVs, most are equipped with cameras, but only the ROVs used by HBU are capable of recording videos. These videos are sonar recordings, which do not plausibly capture identifiable characteristics. The following is a summary of some considerations in assessing this technology:

SPD Unit

SWAT, ABS, & HBU

Technology Use

SWAT and ABS uses ROVs in dangerous situations to assess scenes from a safe position. HBU uses ROVs to perform necessary underwater search and recovery functions. SPD reported that ROVs were used no more than 50 times in 2024. SWAT accounts for the majority of ROV deployments.

Data Sharing

ROV cameras do not capture identifiable information on individuals. There are no captured data relevant to this review.

Data Security

ROV cameras do not capture identifiable information on individuals. There are no captured data relevant to this review.

Potential Civil Liberties Impacts

a. All three units report that warrants were the most common authorization to deploy ROVs in constitutionally protected areas. Each of these units reports that exigent circumstances are "never" or "rarely" used to authorize ROVs.

b. OIG previously found no indication that ROVs are used to observe individuals in a manner that impacts civil liberties or disadvantaged populations.

Internal Assessment

As of January 2025, there have been no new assessments, registered community concerns, or OPA complaints for this surveillance technology.

Costs

All three units reported that there were no significant changes to the cost of ROVs since their acquisition. Their respective inventories of ROVs were acquired prior to 2024; as a result, HBU, SWAT, and ABS reported no costs in 2024.

Recommendations

There are no outstanding or pending recommendations for this technology.

Most recent Compliance Review: Remotely Operated Vehicles (2023)

Forward-Looking Infrared Real-Time Video Camera

The King County Sherriff's Office (KCSO) Air Support Unit monitors several SPD communication frequencies and, if available, assists SPD by providing a helicopter to support patrol, specialized police missions, or search and rescue. KSCO owns two helicopters: Guardian One, which is primarily used for air support for patrol or specialized police missions, and Guardian Two, which is primarily used for search and rescue. Forward-Looking Infrared (FLIR) Real Time Video cameras refers to a camera used in the helicopters that layer heat signatures of individuals and objects on top of the aerial, full-color, 4K resolution video. When using the infrared setting, the FLIR camera allows subjects to be detected even when obscured by clouds, haze, or darkness; however, infrared light cannot penetrate walls or roofs and is not designed to capture details, so the FLIR camera is only able to track subjects outdoors. The following is a summary of some considerations in assessing this technology:

SPD Unit

Multiple units may use FLIR depending on the type of support needed.

Technology Use

In 2024, Guardian One assisted SPD during 134 incidents. As described in prior OIG assessments, it is not feasible to assess how frequently KCSO used the camera or FLIR capabilities on Guardian One.

Data Sharing

SPD can request FLIR video recordings as video evidence from KCSO's Air Support Unit for purposes related to investigations. This evidence can be shared by SPD within legal guidelines or as required by law with agencies, entities, or individuals. Data originate from KCSO Air Support, so SPD rarely receives data sharing requests.

Data Security

SPD mitigates risk to data security by storing evidence in a certified Criminal Justice Information System digital evidence management system that requires all users to be authorized and pass a multifactor authentication barrier. Additionally, in OIG's review of the evidence retained by SPD, individuals were not able to be identified on the stored recordings, which presents low risk to individual data security.

Potential Civil Liberties Impacts

OIG previously found that individuals were not identifiable in evidence retained by SPD. Given the capabilities of this technology, the risk of individuals being identified or targeted beyond the scope of the initial deployment (i.e. bystanders) is low.

Internal Assessment

As of January 2025, there have been no new assessments, registered community concerns, or OPA complaints for this surveillance technology.

Costs

Both the SIR and SPD personnel have stated that the use of FLIR is available to SPD at no charge through the Puget Sound Regional Aviation Project and the Seattle Urban Area Security Initiative.

Recommendations

As of January 2025, one recommendation related to this technology remained open:

1. SPD should amend Policy 6.060 to require that video of demonstrations covered by Seattle Municipal Code 14.12, which are obtained from external entities be sent to the Criminal Intelligence Section or equivalent unit for review within 24 hours and follow the same data retention and destruction timeline as data gathered by department personnel.

Most recent Compliance Review: Forward-Looking Infrared Real-Time Video (2022 & 2023)

Camera Systems

Camera Systems refers to two types of cameras:

- Wires: Concealed on a person and must be activated by that person. When data are recorded on wires, they are recorded locally.
- Fixed Location Cameras: Deployed in public spaces and data are stored on SPD servers. SPD reports that in most cases, the fixed location camera only records when motion is detected. They state the continuous recording setting may be used rarely in the expectation that an event may happen too quickly for motion detection to respond.

The following is a summary of some considerations in assessing this technology:

SPD Unit

TESU supports other units' appropriate and approved requests to use this technology. This process is described in Appendix A of this report.

Technology Use

TESU reported that Camera Systems were deployed 133 times in 2024. This number includes the deployments of both covert and fixed location cameras.

Data Sharing

TESU does not share data with any other entities except for the investigative officer. After extractions take place, all data is removed from the device. While TESU does not share or retain any records, records are possibly shared with other external entities throughout the investigation process by investigative officers.

Data Security

- Wires: TESU extracts data in a secure area where access to this facility is limited to TESU personnel. All evidence from these devices is purged after given to the case detectives.
- Fixed Location Cameras: Data are directly stored on an encrypted server administered by TESU personnel. TESU controls server access, manages data exports, and purges records after evidence is given to case detectives.

Potential Civil Liberties Impacts

The covert nature of Camera Systems raises civil liberty concerns if not used in compliance with Washington State Law or if overused in historically over-policed communities. OIG's prior Compliance Review did not find either of these circumstances to be the case. If camera systems are deployed in an area with an expectation of privacy, the request requires a consent agreement or court order/warrant.

Internal Assessment

As of January 2025, there have been no new assessments, registered community concerns, or OPA complaints for this surveillance technology.

Costs

In 2024, SPD purchased additional cameras and renewed their licensing agreement, resulting in a significant increase in annual costs of $15,173.17.

Recommendations

As of January 2025, one recommendation related to this technology remained open:

1. SPD should develop a process to identify and track all instances when data from Camera Systems are shared with external entities excluding those immediately involved in the criminal justice process.

Most recent Compliance Review: Camera Systems (2023)

Audio Recording Systems

"Audio Recording Systems" refers to covert physical devices (also known as "wires") used to obtain information in criminal investigations. This technology is the base system for the wires identified in the Camera Systems surveillance technology above, except it does not include the video camera attachment. A wire can be deployed on a person, concealed in a space, or disguised within/on objects to capture audio of conversations between identifiable individuals. In almost all cases, at least one participant is unaware of the recording. TESU only approves wire requests when there are few or no other options to obtain evidence, the deployment does not pose an unreasonable risk to the safety of officers and/or corroborating witnesses, and deployment would not reveal the device. The following is a summary of some considerations in assessing this technology.

SPD Unit

TESU supports approved departmental requests to use this technology. TESU's approval process is described in Appendix A of this report.

Technology Use

In 2024, TESU reported that Audio Recording Systems were deployed 31 times.

Data Sharing

TESU does not share data with any other entities except the investigative officer. While TESU does not share or retain any records, it is still possible that these records are shared with other external entities throughout the investigation process by investigative officers.

Data Security

TESU retrieves data from wires by connecting them to a workstation in a secure area where only TESU personnel are authorized to perform extractions. Data are copied to a disc and provided to the investigative officer. After extractions take place, all data are removed from the device, and nothing is retained by TESU. Physical discs containing audio recordings are subject to SPD Policy 7.010, which requires evidence be catalogued with a General Offense number and submitted to the Evidence Unit. The digital recordings may be added to Evidence.com as well, where they are stored indefinitely.

Potential Civil Liberties Impacts

To comply with the Washington Privacy Act, SPD must obtain consent by both parties or obtain a warrant to satisfy consent to deploy Audio Recording Systems. There are rare cases where a warrant may not be necessary if the circumstances satisfy Washington state laws, RCW 9.73.210 or RCW 9.73.230. OIG's prior Compliance Review found that all SPD deployments of Audio Recording Systems were consistent with the Washington State Privacy Act. SPD reported that warrants were the most common type of authorization to deploy Audio Recording Systems in 2024, while consent agreements and exigent circumstances were rarely used as an authorization.

Internal Assessment

As of January 2025, there have been no new assessments, registered community concerns, or OPA complaints for this surveillance technology.

Costs

SPD reported no costs for Audio Recording Devices in 2024.

Recommendations

As of January 2025, one recommendation related to this technology remained open:

1. SPD should develop a process for identifying and tracking all instances when data audio recordings from wires are shared with external entities.

Most recent Compliance Review: Audio Recording Systems (2022)

Computer, Cellphone, and Mobile Device Extraction Tools

Computer, Cellphone, and Mobile Device Extraction (CCMDE) Tools consist of both hardware and software that extract digital information and image the hard drives of devices with proper authorization by consent or search warrant. SPD has multiple different types of CCMDE Tools, but all extract data in a similar manner; using software to bypass, decipher, or disable any password protection. The following is a summary of considerations in assessing this technology:

SPD Unit

ICAC uses this technology for their cases and TESU supports approved departmental requests to use this technology. TESU's approval process is described in Appendix A of this report.

Technology Use

TESU reported that CCMDE tools were deployed 315 times in 2024.

Data Sharing

- ICAC performs internal extractions for their unit and at times performs external data extractions for other law enforcement agencies.
- TESU does not share data with any other entities except for the investigative officer. After extractions take place, all data is removed from the device. While TESU does not share or retain any records, it is still possible that these records are shared with other external entities throughout the investigation process by investigative officers.

Data Security

Both units mitigate risks to data security by ensuring all personnel are certified in CCMDE Tool use, by extracting data in secure locations, by limiting data access to certain personnel, and by only retaining data while an investigation is ongoing.

Potential Civil Liberties Impacts

OIG's most recent Compliance Review found that all SPD deployments of CCMDE Tools received proper authorization. SPD reported that use of CCMDE Tools in 2024 was authorized by warrants or consent agreements, and that exigent circumstances are never used to deploy CCMDE Tools.

Internal Assessment

As of January 2025, there have been no new assessments, registered community concerns, or OPA complaints for this surveillance technology.

Costs

TESU reported that there were no significant changes to cost in 2024. TESU reported that the unit purchased a licensing contract resulting in an increase in cost. TESU reported $120,621.68 in annual costs.

Recommendations

As of January 2025, one recommendation related to this technology remained open:

1. SPD should develop a process for identifying and tracking all instances whenever extracts from Computer, Cellphone, and Mobile Device Extraction Tools are shared with external entities excluding those immediately involved in the criminal justice process associated with the case in which the data were collected.

In 2025, TESU reported they acquired a new software that logs instances of data sharing. Once they use this software, the recommendation will be fully implemented.

Most recent Compliance Review: Computer, Cellphone, and Mobile Device Extraction Tools (2023)

Tracking Devices

Tracking Devices refer to geolocation trackers that transmit location information. Tracking Devices contain both hardware and software elements. The physical device is fixed to a target vehicle and periodically measures GPS coordinates (longitude and latitude), temperature, the device's battery status, and alerts to any tampering, removal, or power shut off. The software translates these data into a map showing locations and movements over time. The following is a summary of some considerations in assessing this technology:

SPD Unit

TESU in support of approved departmental uses of the technology. TESU's approval process is described in Appendix A of this report.

Technology Use

TESU reported that Tracking Devices were deployed 68 times in 2024.

Data Sharing

TESU does not share data with any other entities except for the investigative officer. After extractions take place, all data is removed from the device. While TESU does not share or retain any records, it is still possible that these records are shared with other external entities throughout the investigation process by investigative officers. Once TESU provides the investigative officer the extraction, the disc is the responsibility of the officer. Physical discs are subject to SPD Policy 7.010, which requires evidence be catalogued with a General Offense number and submitted to the Evidence Unit. The digital recordings may be added to Evidence.com as well, where they are stored indefinitely.

Data Security

Data generated during a deployment are encrypted and streamed to a vendor cloud server. TESU personnel control access to the server, managing data exports, and purging all data at the end of the investigation. TESU personnel reported that the vendor agreement forbids the vendor from sharing these data without either authorized consent from SPD or a subpoena from another law enforcement agency.

Potential Civil Liberties Impacts

Deployment of tracking devices requires either a warrant or a consent agreement. Additionally, all requests made to deploy Tracking Devices must comply with Washington State Privacy Act RCW 9.73, Seattle Municipal Code (SMC) 14.12, and TESU must verify that there are no other more feasible evidence collection methods. TESU personnel control inventory and installation of tracking devices and verifies the requesting officer's authorization.

OIG's most recent Compliance Review found that all deployments of Tracking Devices received proper authorization. SPD reported that consent agreements were rarely used to authorize deployments in 2024, while warrants were the most common authorization type to deploy Tracking Devices. Additionally, SPD reported that exigent circumstances are never used to deploy this technology.

Internal Assessment

As of January 2025, there have been no new assessments, registered community concerns, or OPA complaints for this surveillance technology.

Costs

SPD reported no significant costs in 2024, resulting in $27,703.18 in annual costs.

Recommendations

As of January 2025, one recommendation related to this technology remained open:

1. SPD should develop a process for identifying and tracking all instances where data from Tracking Devices are shared with external entities excluding those immediately involved in the criminal justice process associated with the case in which the data were collected.

Most recent Compliance Review: Tracking Devices (2023)

Patrol ALPR

Automatic License Plate Readers (ALPRs) in this report refers to two versions of technology that detect and read characters from license plates for the purpose of locating and recovering stolen vehicles and license plates, to identify vehicles wanted in connection with felonies, to enforce protective orders, and to canvass the area around a crime scene.

- Neology BOSS (Discontinued): A now-decommissioned system of high-definition, infrared digital camera systems that were manually installed in 11 patrol vehicles. Each SPD vehicle equipped with this system had three mounted cameras.
- Axon In-Car Video: As of October 2024, SPD acquired a new licensing agreement that allows them to activate license plate reader capability of the existing in-car video camera systems across the patrol fleet. OIG will assess the use of this new technology for the year 2025.

The following is a summary of some considerations in assessing this technology:

SPD Unit	Patrol
Technology Use	OIG's most recent review of the Neology BOSS ALPR system found more than 8,100 hits that appeared to match a criminal record in 2023. OIG did not update 2024 numbers for this review due to changes in the technology.
Data Sharing	SPD may share data with various external agencies and entities within legal guidelines or as required by law. In OIG's first Compliance Review of Patrol ALPR, SPD reported it did not have a centralized method for sharing ALPR records with external entities. SPD has since updated their ALPR Policy to require the SPD Legal Unit to maintain requests for ALPR data by non-law enforcement or non-prosecutorial agencies. For both versions of ALPR, "Reads," or scans of license plates are stored in a database for 90 days as a resource for investigations.

Data Security

- Neology BOSS: SPD secured the now-decommissioned ALPR database by housing the database in the Seattle Justice Center, where all access what logged and limited to small number of users, and required users to document their justification for searching the database.
- Axon In-Car Video: Data is stored in Evidence.com with similar restrictions that OIG will assess throughout 2025.

Potential Civil Liberties Impacts

OIG's latest review of database use in 2023 found that while SPD Policy 16.170 requires employees to provide case numbers and justification for their searches, about 37% of searches did not provide required documentation. However, OIG found no evidence suggesting that these ALPR searches were used in a manner that impacted civil liberties. This database is expected to grow significantly with expansion to fleet-wide ALPR and will be assessed throughout 2025.

Internal Assessment

As of January 2025, there have been no new assessments, registered community concerns, or OPA complaints for this surveillance technology.

Costs

- Neology BOSS: SPD reported $5,413.28 in licensing costs for use of the system in 2023. There was no additional cost in 2024.
- Axon In-Car Video: SPD reported $357,000 in annual cost for fleet-wide ALPR. These costs include ALPR software, hardware, maintenance, and departmental support.

Recommendations

As of January 2025, one recommendation related to this technology remained open:

1. SPD should develop a process for de-identifying ALPR records released through public disclosure, to the extent allowable under the Washington State Public Records Act.

A second recommendation, 'SPD should develop a strategy for deployment of ALPR-equipped vehicles that takes disproportionality of data collection into account' has been closed now that all SPD patrol vehicles now have ALPR capabilities.

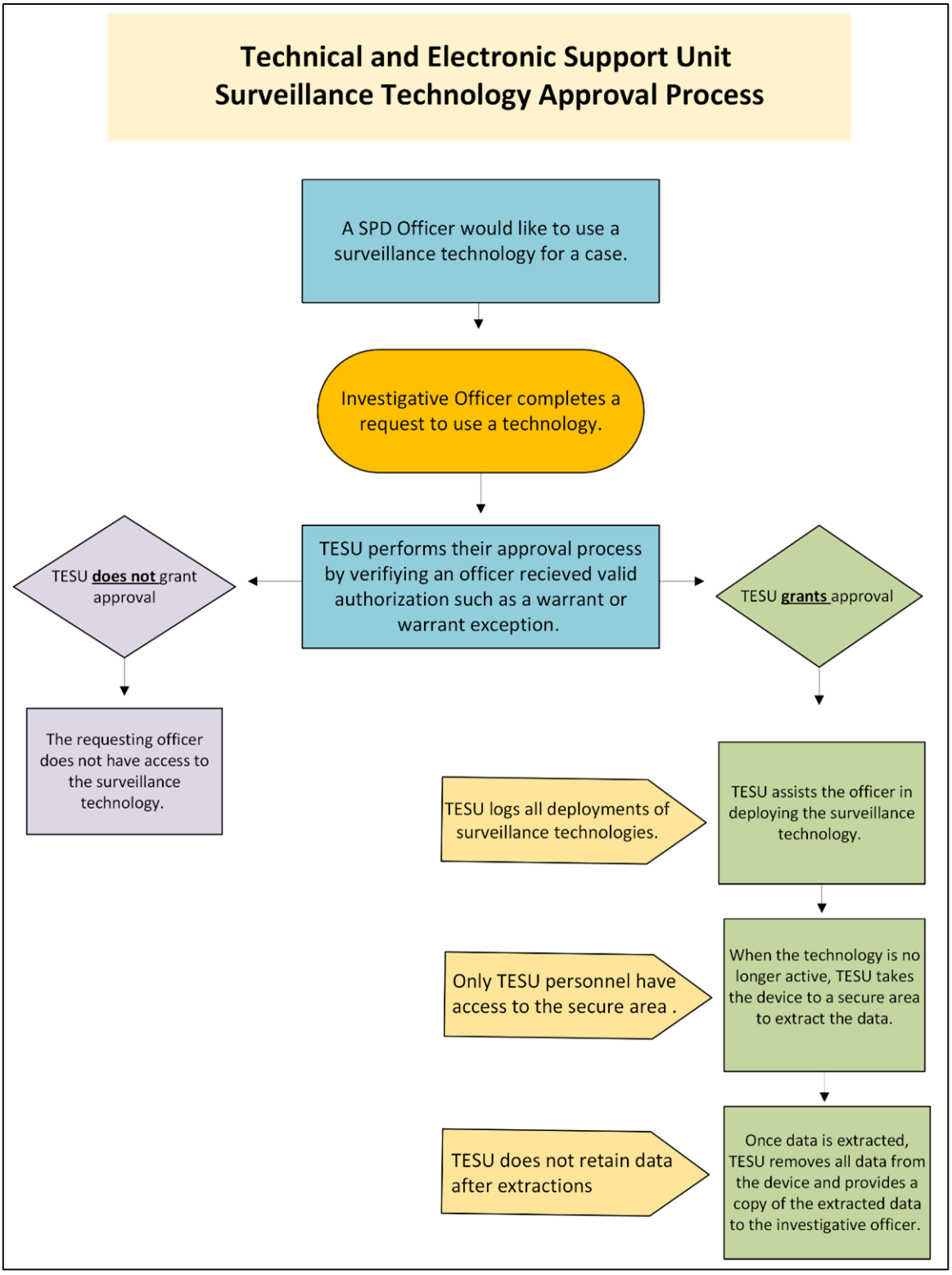
Most recent Compliance Review: Automatic License Plate Readers - Patrol (2023)

Closed-Circuit Television Cameras & Real-Time Crime Center

As a part of Seattle's Technology Assisted Public Safety (TAPS) Program, in addition to the expansion of ALPR, SPD acquired Closed-Circuit Television (CCTV) Systems and Real-Time Crime Center (RTCC) software. Under the pilot program, CCTV is currently limited to four areas within the city (1) Aurora North, (2) Downtown 3rd Avenue Corridor, (3) Belltown, and (4) the Chinatown-International District. CCTV Cameras are the Fusus RTCC software have an expected implementation date of Summer 2025 and there is currently no data for OIG to report.

OIG expects to perform a comprehensive review of these technologies for the duration of the pilot program and report findings in 2026.

Appendix A TESU Approval Process



Appendix B SPD Management Response

The Seattle Police Department appreciates the Surveillance Ordinance audits conducted by the Office of Inspector General. We appreciate the collaboration and support to ensure our department is appropriately using surveillance technology.

Non-Audit Statement This review was not conducted under Generally Accepted Government Auditing Standards (GAGAS); however, OIG has followed GAGAS standards regarding the sufficiency and appropriateness of evidence.