



Seattle Office of
Inspector General

Consolidated Risk Surveillance Usage Review 2025

As Required by Seattle Municipal Code 14.18.060

September 30, 2026

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

206.684.3663
oig@seattle.gov

Table of Contents

Purpose	3
Consolidated Review Methodology.....	4
Relevant Units and Their Roles.....	5
Situational Awareness Cameras Without Recording	6
Remotely Operated Vehicles	7
Camera Systems	8
Audio Recording Systems	10
Callyo.....	12
Computer, Cellphone, and Mobile Device Extraction Tools.....	14
Tracking Devices	16
Parking Enforcement ALPR	18
Hostage Negotiation Throw Phone	19
Forward-Looking Infrared Real-Time Video Camera	20
StarChase.....	22
Appendix A: TESU Approval Process.....	23

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:

- **Technology Use:** frequency and usage patterns
- **Data Sharing:** the frequency and patterns of data sharing
- **Data Security:** how well SPD safeguards individual information
- **Potential Civil Liberties Impacts:** real or possible impacts to civil liberties and any disproportionate impacts on disadvantaged populations
- **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
- **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 to privacy and civil liberty:

- **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.

Consolidated Review Methodology

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

- Situational Awareness Cameras Without Recording
- Remotely Operated Vehicles
- Camera Systems
- Computer, Cellphone, and Mobile Device Extraction Tools
- Audio Recording Systems
- Callyo
- Tracking Devices
- Parking Enforcement Automated License Plate Readers
- Hostage Negotiations Throw Phone
- Forward-Looking Infrared Real-Time Video Cameras
- StarChase

To inform this consolidated review, OIG 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.

Closed Recommendations

OIG closed 12 recommendations pertaining to surveillance technologies during this reporting period. Three recommendations were closed as fully implemented and nine recommendations were administratively closed. These administrative closures were for recommendations that did not address significant risks and were no longer relevant or necessary. OIG will report on the closure of these recommendations in the annual report and on OIG's forthcoming recommendations public dashboard.

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.

Hostage Negotiation Team (HNT)

A specialized unit that responds to crisis incidents, barricaded subjects, or other high-risk operations.

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.

Parking Enforcement (PE)

Responsible for patrolling the city limits, enforcing all parking regulations, and parking violations on city property. These SPD employees also cite abandoned cars, support law enforcement in identifying stolen vehicles, and assist in traffic control in special events or emergencies.

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.

SPD Unit

SWAT

Technology Use

SPD reported Situational Awareness Cameras were used 28 times in 2025. SWAT reports using situational awareness cameras to search for armed/dangerous suspects prior to the SWAT Team entering a space as a safety precaution.

Data Sharing

Situational Awareness Cameras are not used to record images. There are no data available to be shared.

Data Security

Situational Awareness Cameras are not used to record images. There are no data to be safeguarded or stored.

Potential Civil Liberties Impacts

- SWAT reports deployments are commonly pursuant to a warrant, but some deployments are approved through a warrant exception, such as exigent circumstances, consent, or community caretaking.
- 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

There have been no new assessments, registered community concerns, or OPA complaints for this surveillance technology in 2025.

Costs

SWAT reported that there were no significant changes in cost to Situational Awareness Cameras in 2024. The annual cost is approximately \$584.86.

Recommendations

There are no outstanding or pending recommendations for this technology.

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 video. Videos are sonar recordings, which do not plausibly capture identifiable images or characteristics.

SPD Unit

SWAT, ABS, & HBU

Technology Use

SWAT and ABS use ROVs in dangerous situations to assess scenes from a safe position. HBU uses ROVs to perform underwater search and recovery functions. SPD reported ROVs were deployed around 58 times in 2025. 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

- All three units report warrants were the most common method of authorization to deploy ROVs in constitutionally protected areas. Each of these units reports exigent circumstances are “rarely” used to authorize ROVs.
- OIG previously found no indication that ROVs are used to observe individuals in a manner that impacts civil liberties or disadvantaged populations.

Internal Assessment

There have been no new assessments, registered community concerns, or OPA complaints for this surveillance technology in 2025.

Costs

HBU reported \$3,283.00 in repair costs for their unit technology. Both ABS and SWAT reported no costs associated with the technology in 2025.

Recommendations

There are no outstanding or pending recommendations for this technology.

Most Recent Compliance Review:

[Remotely Operated Vehicles \(2023\)](#)

Camera Systems

Camera Systems refers to two types of cameras:

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

SPD Unit

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

Technology Use

TESU reported Camera Systems were deployed 152 times in 2025. This number includes deployments of both covert and fixed location cameras.

Data Sharing

TESU does not share data with any other entities except the investigative officer. While TESU does not share or retain any records, records are possibly shared with other external investigative and prosecutorial entities throughout the investigation process by investigating 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 it is provided 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 misused in historically over-policed communities. OIG's prior Compliance Review did not find either of these circumstances present. 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**

There have been no new assessments, registered community concerns, or OPA complaints for this surveillance technology in 2025.

Costs

In 2025, TESU reported \$10,726 annual costs associated with this technology.

Recommendations

There are no outstanding or pending recommendations for this technology.

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.

SPD Unit

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

Technology Use

In 2025, TESU reported Audio Recording Systems were deployed 34 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, these records are potentially shared with other external investigative and prosecutorial 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, 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 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 all SPD deployments of Audio Recording Systems were consistent with the Washington State Privacy Act. SPD reported warrants were the most common type of authorization to deploy Audio Recording Systems in 2025, while party consent and exigent circumstances were rarely used as an authorization.

Internal Assessment

There have been no new assessments, registered community concerns, or OPA complaints for this surveillance technology in 2025.

Costs

SPD reported no costs for Audio Recording Devices in 2025.

Recommendations

There are no outstanding or pending recommendations for this technology.

Most Recent Compliance Review:

[Audio Recording Systems \(2022\)](#)

Callyo

Callyo refers to a bundle of Motorola Solutions software applications for investigative recording purposes. Callyo provides a variety of applications, each requiring an individual subscription. The Seattle Police Department (SPD) uses three applications: a virtual investigative phone, an audio recording software, and a software that tracks an officer's live location.

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

TESU reported Callyo was used 18 times in 2025.

Data Sharing

TESU only shares data with the investigating officer. Once an investigation has concluded, TESU extracts relevant data, in a secure facility where all access is logged. After extraction, TESU reports all data are removed from the software. While TESU does not share or retain any records, records may be shared with other external investigative and prosecutorial entities throughout the investigation process by investigating officers.

Data Security

Personnel who can grant access to Callyo are limited, providing a control to decrease the likelihood of unauthorized access to or use of the technology. TESU personnel report they delete all Callyo records once evidence has been extracted and preserved. In 2025, TESU reported once data is deleted on their interface at the end of an investigation, the vendor also deletes the corresponding data from their cloud server.

Potential Civil Liberties Impacts

In the most recent compliance review, OIG observed warrants were used in most deployments when an authorization was required to use the technology. Provided that this technology is used in compliance with state law, rarely deployed, and primarily deployed in cases involving child exploitation, OIG does not expect use of this technology to improperly impact civil liberties or have a disproportionate effect on disadvantaged populations.

**Internal
Assessment**

There have been no new assessments, registered community concerns, or OPA complaints for this surveillance technology in 2025.

Costs

TESU reported \$16,327 annual cost of using the technology in 2025.

Recommendations

There are no outstanding or pending recommendations for this technology.

Most Recent Compliance Review:

[Callyo \(2024\)](#)

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 generate an image of the hard drives of devices. Use requires proper authorization by consent or search warrant. SPD has multiple types of CCMDE Tools, but all extract data in a similar manner; using software to bypass, decipher, or disable any password protection.

SPD Unit

ICAC uses this technology for investigations and TESU supports approved departmental requests to use requests for this technology. The TESU approval process is described in Appendix A of this report.

Technology Use

TESU reported CCMDE tools were deployed 315 times in 2025. ICAC reported CCMDE Tools were deployed about 192 times in 2025.

Data Sharing

- ICAC performs internal extractions for their unit and at times performs external data extractions for other law enforcement agencies. ICAC reports 100 instances of data sharing with other law enforcement agencies as the lead investigative unit in the state for internet crimes against children.
- TESU only shares data with the investigating office and not other entities. After extractions take place, all data is removed from the device. While TESU does not share or retain any records, this can occur 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 all SPD deployments of CCMDE Tools received proper authorization. SPD reported use of CCMDE Tools in 2025 was commonly authorized by warrants or consent agreements, and exigent circumstances are rarely used to deploy CCMDE Tools.

**Internal
Assessment**

There have been no new assessments, registered community concerns, or OPA complaints for this surveillance technology in 2025.

Costs

ICAC and TESU reported a combined annual cost of \$497,618 in 2025.

Recommendations

There are no outstanding or pending recommendations for this technology.

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.

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 Tracking Devices were deployed 60 times in 2025.

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 potentially shared with other investigative and prosecutorial entities throughout the investigation process by investigating officers. TESU provides records on a disc to the investigator who assumes responsibility for the data. 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 also be added to Evidence.com 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 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 all deployments of Tracking Devices received proper authorization. SPD reported consent agreements were rarely used to authorize deployments in 2025, while

warrants were the most common authorization type for Tracking Devices. Additionally, SPD reported exigent circumstances are rarely used to deploy this technology.

**Internal
Assessment**

There have been no new assessments, registered community concerns, or OPA complaints for this surveillance technology in 2025.

Costs

SPD reported \$12,625 in annual costs in 2025.

Recommendations

There are no outstanding or pending recommendations for this technology.

Most Recent Compliance Review:

[Tracking Devices \(2023\)](#)



Parking Enforcement Automatic License Plate Readers

Automatic License Plate Readers (ALPRs) are used by both Patrol and Parking Enforcement Officers (PEOs). For Parking Enforcement purposes, PEOs use ALPR to identify parking violations throughout the city. Parking enforcement ALPR can still detect record associated with criminal activity, but PEOs do not conduct enforcement action outside of parking violations.

As of March 2026, Parking Enforcement is no longer using ALPRs until compliance with Senate Bill 6002: Driver Privacy Act can be achieved.

SPD Unit

Parking Enforcement

Technology Use

Parking Enforcement reported ALPR was deployed around 2,026 times in 2025.

Data Sharing

Parking Enforcement reported three requests for data sharing from ALPR. All three requests were from units within the Seattle Police Department.

Data Security

Data collected by PE ALPRs include license plate numbers, read context photos, the date, time and location of the read and the unit performing the read. Personally identifiable information—such as vehicle owner name, address, and phone number— is not stored. SPD Policy 16.170 states PE ALPR reads will be deleted after 24 hours, unless related to hits and data for parking enforcement action. SPD policy and the SIR state hits will be deleted after 90 days unless they are material to a criminal investigation.

Potential Civil Liberties Impacts

In the last compliance review, OIG found PEOs do not often use ALPR data for parking enforcement situations involving people living in their vehicles. The last review also found PE did not have a log documenting ALPR deployment over time, limiting assessments of any potential geographic disproportionalities. However, the Department has since developed this capability.

Internal Assessment

There have been no new assessments, registered community concerns, or OPA complaints for this surveillance technology in 2025.

Costs

Parking Enforcement reported \$73,873.37 annual costs in 2025.

Recommendations

There are no outstanding or pending recommendations for this technology.

Most Recent Compliance Review:

[Automatic License Plate Readers - Parking Enforcement \(2024\)](#)

Hostage Negotiation Throw Phone

The Hostage Negotiation Throw Phone (HNT) refers to the Critical Incident Negotiations Team (CINT) System and tactical phone made by 836 Technologies, used by the SPD Hostage Negotiation team to facilitates two-way communication between law enforcement and a barricaded subject. Facilitating this communication can help officers develop negotiation tactics, conduct a situational assessment, and monitor situational safety.

SPD Unit

Hostage Negotiation Team

Technology Use

HNT did not deploy the Hostage Negotiation Throw Phone in 2025.

Data Sharing

There is no data sharing associated with this technology as it was not deployed in 2025.

Data Security

In the rare case the HNT is used, there is currently one person with as access to the hard drive needed to deploy the technology. When the CINT System is deployed, the system automatically logs and records all calls. The software uses a file type that does not allow users to alter logs, ensuring transparency in the incidents recorded by the system. All data is stored indefinitely and used for HNT training purposes.

Potential Civil Liberties Impacts

Deployment into a constitutionally protected area requires warrant or warrant exception such as consent, exigent circumstances, or community caretaking/emergency. In the latest review of this technology published in 2025, OIG found all deployments of Hostage Negotiation Throw Phone received proper authorization.

Internal Assessment

There have been no new assessments, registered community concerns, or OPA complaints for this surveillance technology in 2025.

Costs

SPD reports no cost associated with this technology in 2025.

Recommendations

There are no outstanding or pending recommendations for this technology.

Most Recent Compliance Review:

[Hostage Negotiation Throw Phone Report \(2024\)](#)

Forward-Looking Infrared Real-Time Video Camera

The King County Sheriff'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. KCSO owns two helicopters: Guardian One, primarily used for air support for patrol or specialized police missions, and Guardian Two, mostly used for search and rescue. "Forward-Looking Infrared (FLIR) Real-Time Video Cameras" refers to a camera used in the helicopters that layers 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.

SPD Unit

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

Technology Use

In 2025, Guardian One assisted SPD during 119 incidents. As described in prior OIG assessments, it is not feasible to assess whether or how frequently KCSO used the camera or FLIR capabilities when deploying Guardian One.

Data Sharing

SPD can request FLIR video recordings as video evidence from KCSO's Air Support Unit for 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 identifiable on the stored recordings, presenting low risk to individual data security.

Potential Civil Liberties Impacts

OIG previously found individuals were not identifiable in evidence retained by SPD. Given the limited 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

There have been no new assessments, registered community concerns, or OPA complaints for this surveillance technology in 2025.

Costs

Both the SIR and SPD personnel have stated 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

There are no outstanding or pending recommendations for this technology.

Most Recent Compliance Review:

[Forward-Looking Infrared Real-Time Video \(2022 & 2023\)](#)

StarChase

In June 2025, City Council approved a material change in the Track Devices Surveillance Impact Report to include remotely deployable GPS trackers, called StarChase. StarChase is a tool designed to tag and track fleeing vehicles as police pursuit management technology. SPD reported an intention to use StarChase as a pursuits tactic in accordance with RCW 10.116.060.2.d. requiring police departments to “develop a plan to end the pursuit through the use of available pursuit intervention options.”

While StarChase was approved for use in 2025, SPD has not deployed the technology. OIG will conduct a comprehensive technology review when SPD deploys StarChase.

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.

Appendix A TESU Approval Process

Technical and Electronic Support Unit Surveillance Technology Approval Process

