



Seattle Office of Inspector General

Surveillance Technology Usage Review: Forward Looking Infrared Real-Time Video (2021)

As Required by Seattle Municipal Code 14.18.060

April 28, 2023

Office of Inspector General
City of Seattle
PO Box 94764
Seattle, WA 98124-7064
oig@seattle.gov
(206) 684-3663

Foreword from the Inspector General

Enclosed is OIG's first Annual Surveillance Usage Review on the use of Forward Looking Infrared Real-Time Video (FLIR) by the Seattle Police Department (SPD). This review was performed pursuant to Seattle Municipal Code 14.18.060, which specifies that OIG conduct annual reviews of SPD's use of Surveillance Technologies. FLIR is one of sixteen SPD Surveillance Technologies currently approved by City Council.

OIG contracted with cybersecurity firm Critical Insight to conduct this review, and we thank them for their work, as well as their ongoing partnership in overseeing SPD's use of approved Surveillance Technologies.

Throughout this process, OIG directed and reviewed the work of Critical Insight. OIG also facilitated stakeholder feedback from SPD, the American Civil Liberties Union, and City Council staff. We appreciate the time and effort these stakeholders devoted to this review. These consultations and perspectives helped to ensure the work was thorough and inclusive, and that our conclusions and recommendations are based on the most complete information available.

In performing this review annually, OIG will continue to engage with SPD and other stakeholders to ensure responsiveness to community concerns and innovate in the area of evaluating how SPD uses Surveillance Technologies to further public safety while protecting the rights of individuals in our community.



Critical Insight

CITY OF SEATTLE SURVEILLANCE TECHNOLOGY REVIEW FORWARD LOOKING INFRARED REAL- TIME VIDEO (FLIR)

SOW-2022-271

APRIL 28, 2023

Notice

Critical Insight has made every reasonable attempt to ensure that the information contained within this statement of work is correct, current and properly sets forth the requirements as have been determined to date. The parties acknowledge and agree that the other party assumes no responsibility for errors that may be contained in or for misinterpretations that readers may infer from this document.

Trademark Notice

2022 Critical Insight, Inc. dba CI Security. All Rights Reserved, CI Security®, Critical Insight™, the Critical Insight and Kraken logos and other trademarks, service marks, and designs are registered or unregistered trademarks of Critical Insight in the United States and in foreign countries.

© Copyright 2023 Critical Insight, Inc.




Table of Contents




Executive Summary	4
Summary of Assessments and Recommendations Related to SMC 14.18.060	4
Purpose and Objectives	6
Technology Description	6
A. Surveillance Technology Usage	9
Patterns of Use	9
Purpose of Use	12
B. Data Sharing with External Entities	13
C. Data Management and Safeguarding of Individual Information	14
Secure Storage and Access	14
Data Retention	15
D. Impact on Civil Liberties and Disproportionate Effects on Disadvantaged Populations	16
Bystander Anonymity	16
Video of Protests and Demonstrations	16
Disproportionate Effects on Disadvantaged Populations	17
E. Complaints, Concerns and Other Assessments	20
F. Cost Auditing	20

Executive Summary

This Executive Summary highlights our major findings and recommendations pertaining to the six elements of SMC 14.18.060, which structures OIG’s review. The summary below lists our significant audit results associated with SMC 14.18.060.

Summary of Assessments and Recommendations Related to SMC 14.18.060

14.18.060 Provision	Compliance Determination	Auditor’s Findings	Recommendations
A. How surveillance technology has been used, usage frequency, and whether usage patterns have changed.	Yes 	<p>Current policy gives SPD tactical flexibility in responding to a wide variety of emergency situations with minimal delay, which we believe is reasonable given the wide range of potential life-safety circumstances that may require it. No overuse or misuse was identified but monitoring should be ongoing.</p>	
B. How often surveillance technology or its data is shared with other entities, including government agencies.	Yes 	<p>SPD does not generally share FLIR video with partners external to the City because the video originates from KCSO. Video may be requested through Public Records Requests.</p>	
C. How well data management protocols are safeguarding individual (personal) information.	Needs Work 	<p>SPD and Seattle IT personnel identified that the city is not performing regular access audits of the digital evidence management system where video recordings taken from KCSO FLIR are stored.</p> <p>SPD personnel identified no formal, routine procedure for reviewing user accounts to ensure that account holders are still authorized to access to the digital evidence management system</p>	<p>No recommendations toward these findings at this time, as the system, policies, and processes addressed in these findings are broader than the scope of this technology review. OIG will continue to monitor this concern and explore potential follow-up work to address the systemwide concerns.</p>

14.18.060 Provision	Compliance Determination	Auditor's Findings	Recommendations
		<p>where video recordings taken from KCSO FLIR are stored.</p>	
<p>D. How deployment of surveillance technologies impacted or could impact civil liberties or have disproportionate effects on disadvantaged populations, and how those impacts are being mitigated.</p>	<p>Needs Work</p> 	<p>Videos provided by KCSO may include non-FLIR footage in which individual faces and vehicle markings are clearly visible. The process of anonymizing the identities of bystanders prior to external release of the video is not clear.</p> <p>SPD policy is unclear whether video or photographs of demonstrations protected under Seattle Municipal Code 14.12, which are provided by KCSO, are subject to vetting and purging as outlined in SPD policy 6.060.</p>	<p>Recommendation 1 SPD should clarify in the SIR the process for protecting bystanders' identities when sharing footage or images from KCSO's Arial Support Unit in response to a Public Records Request.</p> <p>Recommendation 2 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.</p>
<p>E. A summary of any complaints or concerns about the surveillance technology and results of internal audits or assessments of code compliance.</p>	<p>Yes</p> 	<p>Our review found no complaints related to the use of FLIR on KCSO helicopters.</p>	
<p>F. Total annual costs for use of surveillance technology, including personnel and other ongoing costs.</p>	<p>Yes</p> 	<p>The SIR and SPD identify that KCSO air assets can be called out at no cost to SPD through the Puget Sound Regional Aviation Project</p>	

Technology Description

The King County Sheriff's Office (KCSO) Air Support Unit is the only full-time rotary-wing law enforcement aviation unit in Washington State. Three separate helicopters, one Bell 206B3 helicopter, one UH-1H "Huey," and one Bell 407, operate as Guardian One and Guardian Two. The Air Support Unit operates throughout King County and is available to assist the Seattle Police Department at no charge through the Seattle Urban Area Security Initiative (UASI) and the Puget Sound Regional Aviation Project, a consortium made up of members from sheriff's offices in King, Snohomish, Pierce, and Kitsap counties as well as Seattle Police and Fire departments, Pierce County Fire Districts, Washington State Patrol, the Department of Emergency Management in Pierce County, the Washington State Department of Ecology, US Coast Guard, US Navy, and the National Park Service.

Guardian One offers air support for patrol and specialized police missions. Guardian Two offers support predominately for search and rescue. These helicopters are equipped with color and forward-looking infrared cameras and 30 million-candle power (equivalent to 377 million lumens) spotlights that enable the location of suspects or disaster victims in darkness or environmental cover.

The Air Support Unit (KCSO) monitors several SPD communication frequencies and if available to assist, advises SPD communications that Guardian One is available to support. In life, safety, or other serious crime incidents where air support would be beneficial, SPD sergeants and/or higher ranked personnel may request the assistance of the Air Support Unit. Guardian Two is available as a call-out resource in the event of a significant incident.

The aerial vantage point created via the use of helicopters helps trained law enforcement personnel provide enhanced vision to locate and track the movement of crime suspects and disaster victims. The FLIR camera technology housed within the Guardian One and Guardian Two helicopters provides a further enhanced picture of incident scenes by layering heat signatures of individuals and objects on top of the aerial video. The FLIR technology allows for subjects to be detected even when obscured by clouds, haze, or darkness; however, infrared light cannot penetrate walls or roofs, so the FLIR camera is only able to track subjects outdoors.

Purpose and Objectives

The purpose of this document is to communicate the findings of an analysis of the Surveillance Impact Report (SIR) and associated departmental policies and processes for the Seattle Police Department's use of the helicopter-mounted Forward Looking Infrared (FLIR) camera aboard the Guardian One and Guardian Two helicopters operated by King County Sheriff's Office (KCSO) under a mutual-aid agreement.

This analysis was conducted by Critical Insight consultants at the request of the Office of the Inspector General for Public Safety at the City of Seattle under City Ordinance 125376, under Chapter 14.18.060, which requires an annual review of actual usage of surveillance technologies by the Seattle Police Department (SPD). Per Ordinance 125376, this review is required to include, but is not limited to, the following:

- A. How surveillance technology has been used, how frequently, and whether usage patterns are changing over time;
- B. How often surveillance technology or its data are being shared with other entities, including other governments in particular;
- C. How well data management protocols are safeguarding individual information;
- D. How deployment of surveillance technologies impacted or could impact civil liberties or have disproportionate effects on disadvantaged populations, and how those impacts are being mitigated, including, for SPD, an examination of whether deployments are pursuant to warrants or not and how SPD's surveillance technology is used to analyze patterns to predict suspect, individual, or group-affiliation behavior;
- E. A summary of any complaints or concerns received by or known by departments about their surveillance technology and results of any internal audits or other assessments of code compliance; and
- F. Total annual costs for use of surveillance technology, including personnel and other ongoing costs.

In the course of this review, consultants reviewed the information disclosed in the SIR, as well as Seattle Police Department policy relating to evidence handling, video surveillance and bias-free policing, and reviewed case notes and recordings associated with all known callouts of Guardian One and Guardian Two where SPD

was involved during calendar year 2021. This review also included a survey of concerns raised by the Privacy and Civil Liberties Assessment and Public Comment sections of the SIR.

This report will highlight risks discovered by Critical Insight consultants in the following areas, and give recommendations on how to remediate those risks:

- Is the description of the technology in the SIR complete and accurate?
- Is there a clear usage and data management policy or policies in place?
- Does the SIR and/or policy describe how and when the surveillance technology will be deployed, and by whom?
- How and where will data gathered by this surveillance technology be stored?
- How long will the data be retained for?
 - What process is used to destroy data that are no longer being retained?
- How is access to the data secured?
 - How is unauthorized access prevented?
 - What access reviews are being performed?
- How are data shared outside of the department, and how is sharing or access to those data monitored and audited?
- Are there any auditability concerns about the technology, its cost, and its usage in general?
 - Example: Instances where access authorization cannot be reviewed because log data are not available.
 - Example: Instances of the use of a particular surveillance technology not being tagged properly in case notes.

A. Surveillance Technology Usage

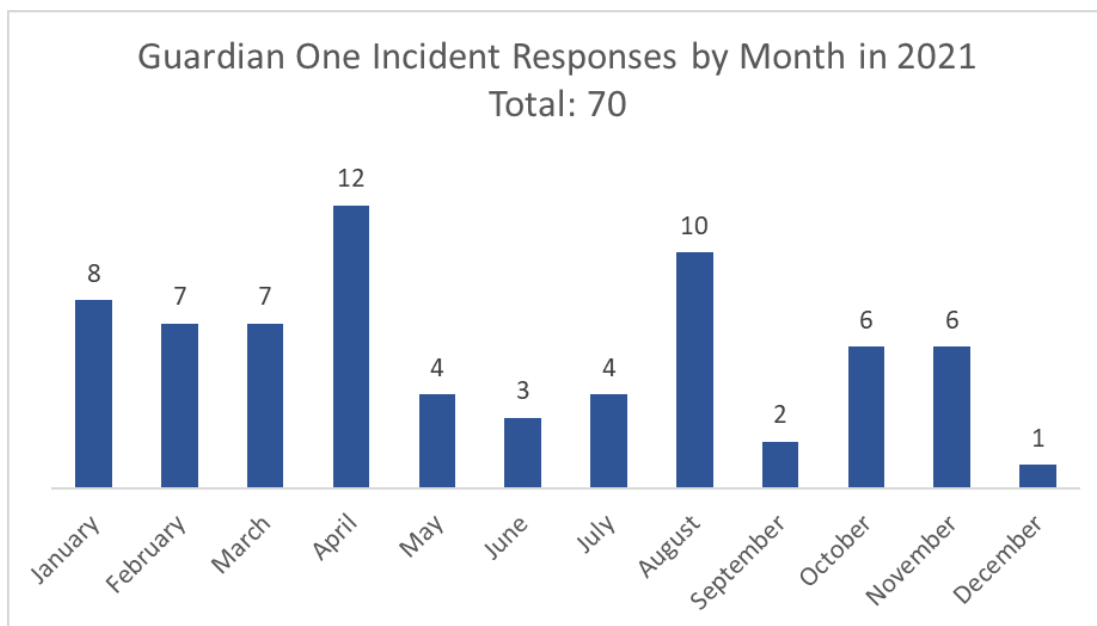
As part of this review, Critical Insight attempted to identify all instances when KCSO helicopters equipped with FLIR technology assisted SPD in 2021. This review included instances when SPD requested KCSO support and when KCSO initiated a response.

We were unable to separate instances when the FLIR technology was used from those in which it was not. This is because SPD data only specify when a helicopter responded to an incident and not when the FLIR technology was used during a given deployment; moreover, SPD does not possess most video recorded by KCSO helicopters.¹ While it is unclear how many deployments of KCSO helicopters in support of SPD involved the use of FLIR technology, we note that community concerns documented in the SIR along with statistics of overflights provided by SPD go beyond SPD’s use of FLIR and into general use of KCSO helicopters.

No callouts involving Guardian Two were found during our review of FLIR activity in calendar year 2021. All 70 callouts from the 2021 calendar year involved Guardian One.

Patterns of Use

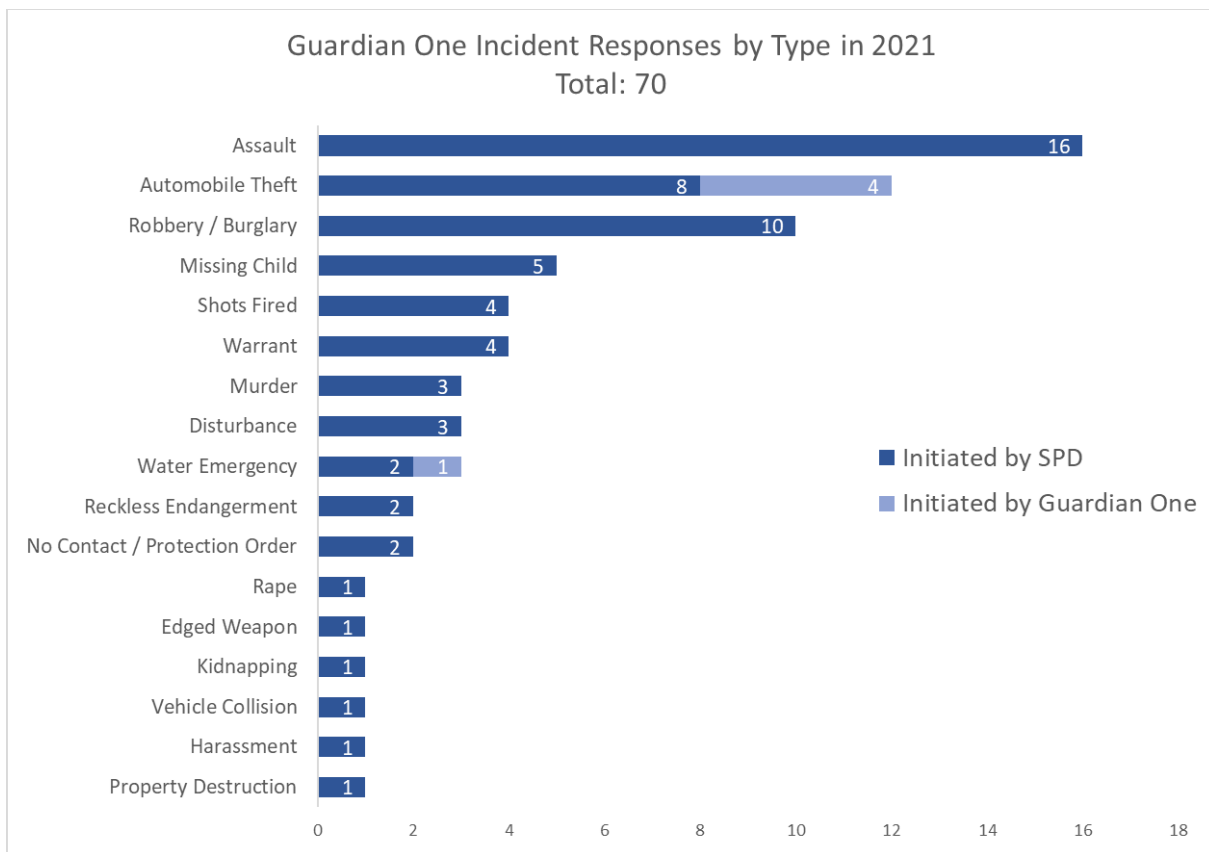
We found that Guardian One was involved in 70 SPD incident responses during 2021:



¹ See Section B of this report for more discussion of how and when SPD obtains video from KCSO.

Of these, 5 callouts were initiated by Guardian One in response to activity its crew observed and relayed to SPD. Based on our review of Computer-Aided Dispatch (CAD) records, the remaining 65 incident responses appear to have been initiated by SPD. Included in these SPD responses are instances when Guardian One offered support to SPD operations as a result of monitoring SPD communications. Guardian One was not always available when SPD requested it. We identified that on at least 9 occasions SPD requested Guardian One’s assistance, but the helicopter was unavailable.

Guardian One responded to the following types² of incidents in 2021:



Within the review period, we did not find any law or policy which required a warrant for use of FLIR or KCSO helicopters. In the SIR, community members raised concerns about continuous or targeted surveillance of Seattle residents by KCSO helicopters and/or the FLIR technology. We did not find any evidence that these technologies were used for these purposes or to analyze patterns or predict behavior of individuals or groups.

² Incident types are based on the final disposition of the incident, and grouped for analysis.

To illustrate some ways in which Guardian One has been involved in incident responses, we provide a randomly selected sample of incidents that Guardian One responded to in 2021 and brief descriptions of the helicopter's role in those incidents as reflected by SPD records.³

Missing Child

A 6-year-old child was reported missing. Guardian One arrived on scene 20 minutes after dispatch and checked parks and schools within the search area. Child was located approximately 10 minutes later.

Assault

A security employee reported that an unidentified suspect fired multiple shots at him. Guardian One arrived on scene 2 minutes after dispatch and searched for the suspect but was unable to locate them.

Property Destruction

Officers responded to reports that a vehicle was fired at while occupied, shattering the window. Guardian One was dispatched but CAD records were unclear if it arrived on scene. Officers were unable to obtain information about the suspect or the vehicle they were driving, and it was determined by officers that a rock shattered the window.

Automobile Theft

Officers identified a car as stolen. The driver of the vehicle fled in it, and officers were unable to maintain visual contact. Guardian One was dispatched to aid in the search but was unable to find the car.

Edged Weapon

Officers responded to reports that a subject was swinging a sword outside of a business. Guardian One was dispatched to help search for the subject, but he was contacted by officers on scene and found not to be a threat. The reported sword was made of foam.

Reckless Endangerment

³ CAD is the primary source of information related to listed incidents. Records of the timing and extent of Guardian One's involvement may vary in detail from incident to incident.

Guardian One joined the call of an ongoing arrest by an SPD street racing detail to advise that there was a large group nearby (possibly engaging in street racing).

Murder

Officers responded to reports of a shooting. As officers attempted to locate the suspect, Guardian One was dispatched to aid the search. Officers appear to have contacted the suspect and exchanged fire before Guardian One's arrival. As officers attempted to treat the suspect, Guardian One then began searching for victims nearby.

Robbery/Burglary

Officers responded to a call from a security company employee who found individuals burglarizing a vacant building. The employee observed the suspects leaving in a vehicle. Guardian One was dispatched, but on-scene officers found the suspects' vehicle stopped nearby and arrested the suspects.

Purpose of Use

Policy 16.060 – “King County Sheriff’s Office Air Support Unit” of the Seattle Police Department Manual states that “Guardian One offers air support for patrol and specialized missions” and that “Guardian Two offers air support for special operations such as search and rescue (SAR) and tactical missions.” This policy and the SIR describe the process by which SPD may request support from KCSO’s Air Support Unit and provides types of events to which Guardian One previously responded; neither SPD policy nor the SIR give specific parameters describing what responses should involve KCSO helicopter support. The Surveillance Impact Report for FLIR does state that “in life safety, or other serious crime incidents where air support would be beneficial, SPD sergeants and/or higher ranked personnel may request the assistance of the Air Support Unit.”

This request process, and the fact that authority to request KCSO helicopter assistance is granted to a relatively large number of SPD officers, gives SPD tactical flexibility in responding to a wide variety of emergency situations with minimal delay. While Critical Insight did not observe overuse or misapplication within the cases we reviewed, and as a result are not making a recommendation at this time, the role of the KCSO Air Support Unit should continue to be monitored in future reviews.

B. Data Sharing with External Entities

The SIR states that SPD can request FLIR video recordings made by Guardian helicopters as video evidence from KCSO's Air Support Unit for purposes related to investigations. The SIR further states that SPD may share video evidence with the following agencies, entities, or individuals within legal guidelines or as required by law:

Seattle City Attorney's Office

- King County Prosecuting Attorney's Office
- King County Department of Public Defense
- Private Defense Attorneys
- Seattle Municipal Court
- King County Superior Court
- Similar entities where prosecution is in Federal or other State jurisdictions
- Members of the public pursuant to the Washington Public Records Act, Chapter 42.56 RCW

SPD personnel informed us they generally do not receive requests from external partner agencies for FLIR video evidence. According to SPD, these agencies are aware these videos originate from KCSO's Air Support Unit and that SPD is a consumer of this information. Therefore, requests for FLIR videos are often submitted directly to KCSO, not SPD. The only time this may differ would be in the context of litigation involving the City, in which video stored by SPD would be shared with other agencies in response to discovery requests.

Cases involving KCSO air assets were reviewed to identify whether FLIR video evidence was obtained from KCSO's Air Support Unit in 2021. Our review did not find any FLIR videos from that year stored within SPD systems. This supports a reasonable conclusion that SPD did not share any FLIR video evidence from 2021 with external partner agencies or through a public records request. However, according to SPD personnel, FLIR video evidence from prior years was shared with the City Attorney's Office during calendar year 2021. SPD advised that this evidence was attorney-client privileged.

C. Data Management and Safeguarding of Individual Information

Critical Insight conducted a review of storage and access procedures and capabilities used to safeguard the privacy and personal information of anyone who may be identifiable in videos provided by KCSO's Air Support Unit. While acknowledging that such videos constitute a minute proportion of data SPD stores within Evidence.com⁴, we provide the following concerns related to the safeguarding of data within the system:

Secure Storage and Access

While all user sign-ins to the Evidence.com platform do pass through the City's Active Directory instance and are reviewed for signs of impossible travel by Seattle IT and its managed security vendor, we found that once users log into the Evidence.com platform, patterns of user activity on Evidence.com are not actively monitored for potential threat indicators. We found that neither SPD nor Seattle IT are consuming or utilizing Evidence.com's access and audit logs, which Evidence.com makes available via a web Application Programming Interface (API) for this reason. This logging and audit API could allow Seattle IT to monitor Evidence.com for patterns of use which could indicate threat actor activity such as theft of data.

While the City has a contract with cybersecurity managed services provider Mandiant, access and audit logs from Evidence.com are not currently being imported into Mandiant's MDR platform.⁵ Since Evidence.com is a Software-as-a-Service (SaaS) platform, and exists outside of the City network, the City cannot use its internal netflow data to identify potential data exfiltration events.

We also found that account access authorization reviews are not being regularly performed on Evidence.com user accounts. During interviews with SPD and Seattle IT personnel, we asked whether individual Evidence.com accounts are ever reviewed to ensure that the account holder is still authorized to access Evidence.com on behalf of SPD. We were told that while accounts are disabled and access is removed when individuals leave their jobs or change job responsibilities, there is no formal, routine

⁴ SPD's answer to Section 5.1 of the SIR regarding secure storage of data does not refer to Evidence.com specifically, but states "The SPD Evidence Unit stores the video in the CJIS certified Digital Evidence Management System (DEMS)". Evidence.com is SPD's current CJIS-certified digital evidence management system.

⁵ The industry standard remedy for this risk is to feed audit log data from the SaaS system into a Security Information and Events Management (SIEM) system or a Managed Detection and Response (MDR) platform such as the City's existing Mandiant solution.

procedure to review accounts. A formal access review process is an industry standard best practice and is recommended by all major security governance frameworks, including the NIST Cybersecurity Framework,⁶ a set of guidelines and recommendations published by the US National Institute of Standards and Technology that is widely regarded as the default security framework for individual businesses and state and local government. Regular account reviews are considered essential for safeguarding private and confidential information because threat actors routinely make use of “stale” accounts belonging to individuals who have left an organization but whose access remains active.

Critical Insight is not making recommendations at this time, as the systems, policies, and processes addressed in these findings are broader than the scope of this technology review. OIG will continue to monitor this concern and explore potential follow-up work to address the systemwide concerns.

Data Retention

According to SPD personnel, no data are currently deleted or removed from Evidence.com. The current policy of indefinite retention does not conflict with retention periods set by the Washington State Law Enforcement Records Retention Schedule, as those retention periods only establish minimums.

⁶ <https://www.nist.gov/cyberframework>

D. Impact on Civil Liberties and Disproportionate Effects on Disadvantaged Populations

Bystander Anonymity

While the FLIR camera itself does not produce images in which individuals are identifiable, the FLIR sensor package also contains a visible-light mode that provides full-color 4K-quality video in which individual faces and vehicle markings are clearly visible. The crew of the helicopter can toggle between full-color and FLIR views at any time, and when the crew switches to full-color mode, this change is reflected in the video recording that may later be made available to SPD.

As a result, it is still possible to identify individuals captured in FLIR video if the crew switches the view mode to full color. The FLIR SIR does not directly quote or include policies regarding how SPD redacts or deletes information when sharing FLIR data through a public records request. Section 6.0 of the SIR does state that “applicable exemptions” will be applied to the data before disclosing to a requestor, but neither the SIR nor department policy elucidate what these exemptions might be or how they are applied.⁷

- **Recommendation 1:** SPD should clarify in the SIR the process for protecting bystanders’ identities when sharing footage or images from KCSO’s Aerial Support Unit in response to a Public Records Request.

Video of Protests and Demonstrations

Community members raised concerns in the SIR about the use of KCSO helicopters to surveil demonstrations and the data collected from that observation. As discussed in Section A of this report, SPD policy 16.060 does not restrict the types of incidents to which KCSO helicopters can be asked to respond. SPD policy also does not constrain the independent activities of the KCSO Air Support Unit or what KCSO does with the data they collect.

SPD policy does place protections on what the Department does with videos and photographs taken at demonstrations in compliance with Seattle Municipal Code

⁷ We note that KCSO Air Support Unit posts FLIR videos on its YouTube channel, including of instances where they are assisting SPD. However, we found no such videos of SPD incidents in 2021. KCSO processes for protecting bystanders’ identities are outside the scope of this review.

14.12 – “Collection of Information for Law Enforcement Purposes”. SPD Manual section 6.060 states:

10. Criminal Intelligence Section Receives and Vets Original Copies of all Videos and Photographs Taken at a Demonstration Covered by the Ordinance
Employees will send original copies of all videos and photographs taken at a demonstration to the Criminal Intelligence Section within 24 hours of the event.

Employees will not make or retain any copies of these videos and photographs. Within five days of the demonstration, the Criminal Intelligence Section will purge all videos and photographs not covered by an authorization to be retained.

Exception: This section does not apply to in-car and body-worn video.⁸

Notably, this policy appears to only speak to original copies of photographs and videos taken by SPD personnel. It is unclear if this policy applies to copies of video or photographs received from external entities.⁹

The SIR provides that SPD investigators may request video from KCSO’s Air Support Unit only “when the video will be entered as case evidence in the investigation of a crime or missing person.” While this reported practice mitigates risk of SPD retaining video of lawful demonstrators, there may be instances where footage of isolated unlawful behavior includes identifiable images of lawful protestors and bystanders. This consideration is why all videos and photographs of relevant demonstrations are routed to the Investigative Support Unit for vetting and tracking.

We recommend amending the SPD Manual to more clearly cover video evidence gathered by KCSO:

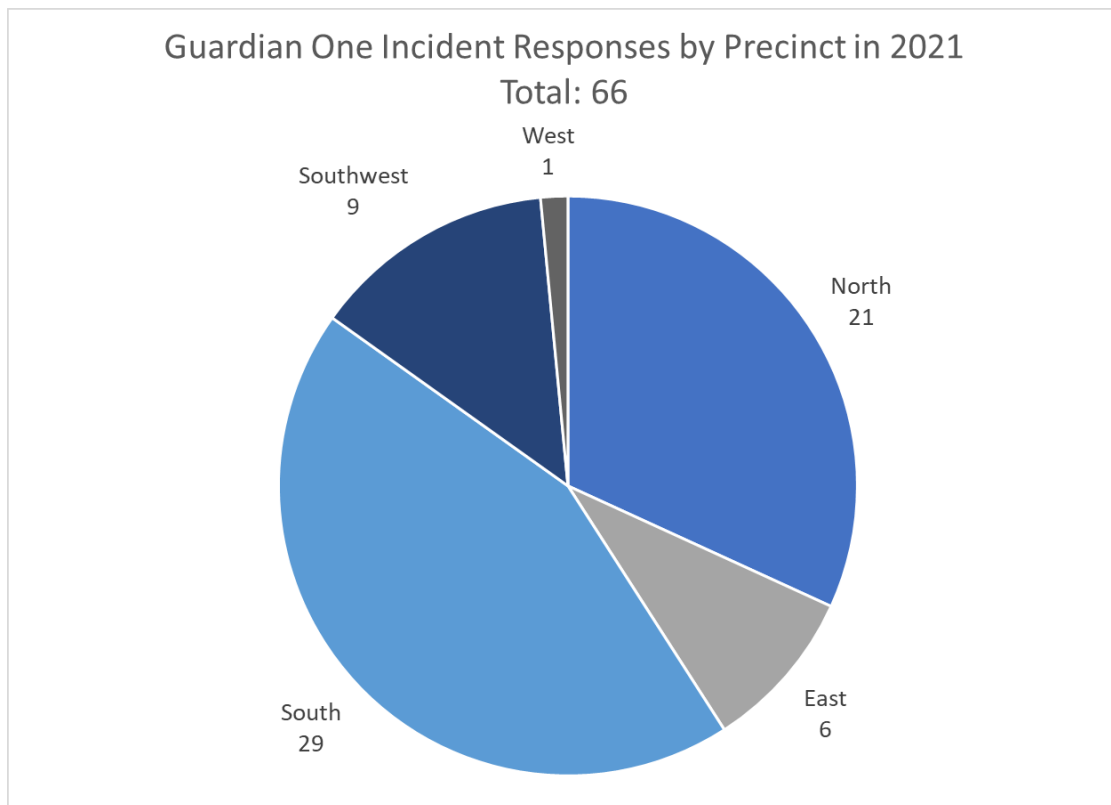
- **Recommendation 2:** SPD should amend Policy 6.060 to require that video of demonstrations covered by Seattle Municipal Code 14.12, which are obtained from external entities, be sent to the Criminal Intelligence Section or equivalent unit for review within 24 hours and follow the same data retention and destruction timeline as data gathered by department personnel.

Disproportionate Effects on Disadvantaged Populations

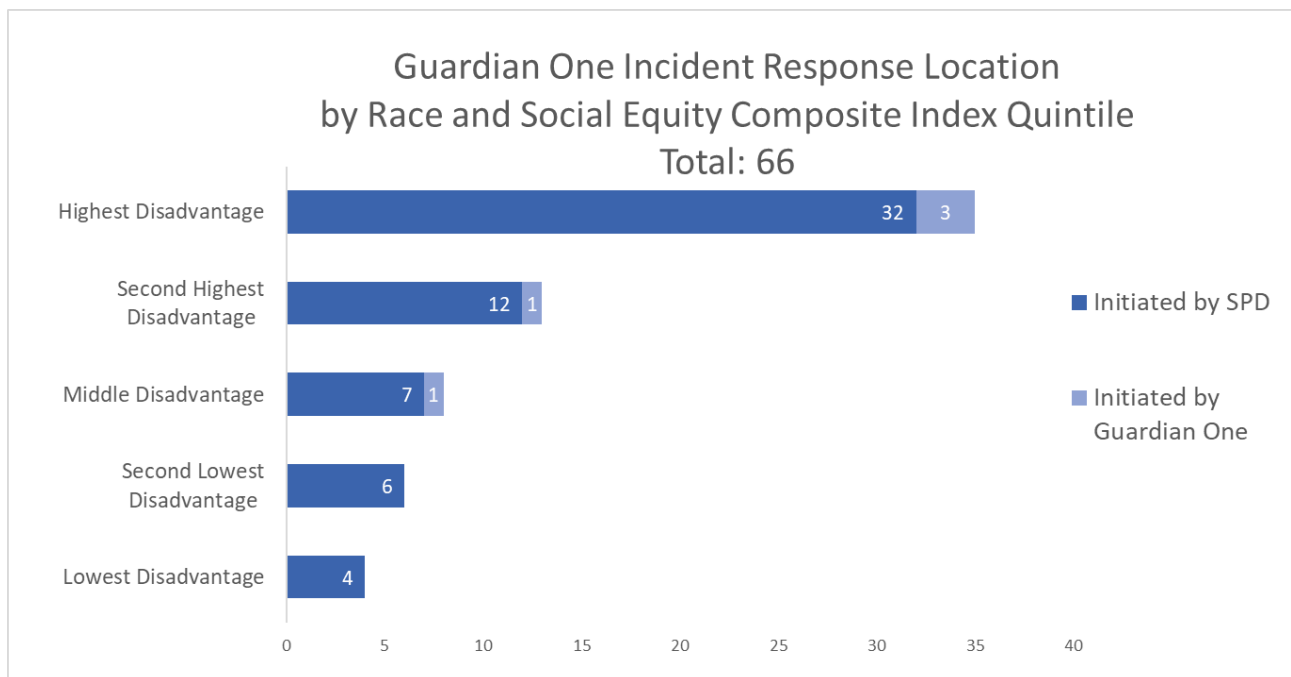
⁸ Policy 6.060 refers to the Criminal Intelligence Section, however SPD has provided that this function is now fulfilled by the Investigative Support Unit.

⁹ SPD Manual section 7.090-POL-3 outlines how employees may accept photos from outside entities, but does not provide for routing of applicable materials to the Investigative Support Unit.

As part of this review, we evaluated addresses where Guardian One responded to an incident for potential disproportionality. We found that 76% of Guardian One incident responses within Seattle were concentrated in two precincts: North and South. We exclude four responses initiated by SPD from the chart below because Guardian One ultimately responded to a location outside of Seattle.



In order to examine the extent to which helicopters responded to locations in disadvantaged communities, we compared Guardian One response addresses to the City of Seattle’s Racial and Social Equity Composite Index map¹⁰. As shown below, greater-than-half of Guardian One responses in 2021 appear to have been to incidents in neighborhoods which are at the greatest disadvantage.¹¹



For 2021, Guardian One disproportionately responded to communities already considered at the greatest disadvantage. This is noteworthy because frequent helicopter overflights may impact citizens’ sense of safety in the places where they live, and because frequent helicopter overflights at low altitude may disrupt sleep at any time of day or night due to the prevalence of shift and gig work as forms of employment in disadvantaged communities. However, because Guardian One typically responds to incidents already in progress we cannot draw conclusions about

¹⁰ The Racial and Social Equity Index is a census-tract based tool compiled in 2018 by the City of Seattle Demographer in the Office of Planning and Community Development. The index combines the three equally weighted sub-indices (Race, English Language Learners, and Origins sub-index, Socioeconomic Disadvantage sub-index, and Heath Disadvantage sub-index), with census tracts categorized by five levels (quintiles) of priority/disadvantage. <https://www.arcgis.com/home/webmap/viewer.html?panel=gallery&layers=225a4c2c50e94f2cb548a046217f49f7>

¹¹ This analysis is based on the location of an incident. In some cases, Guardian One may have been dispatched and in-route at the time the incident was resolved.

disparity in use of the helicopter without a broader review of police deployment and responses.

E. Complaints, Concerns and Other Assessments

Office of Police Accountability (OPA) Complaints

We found no complaints submitted to OPA regarding the FLIR surveillance technology in 2021.

Customer Service Bureau Complaints

We found several complaints from 2021 about helicopter noise late at night. One was a potential noise complaint related to the FLIR-equipped helicopters, while the other complaints were not clearly identified as belonging to law enforcement.

Internal Audits or Assessments

According to SPD's Audit, Policy, and Research Section, no internal audits or assessments have been conducted on this technology.

F. Cost Auditing

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 (UASI).

RECOMMENDATION RESPONSES FROM SPD

1. SPD should clarify in the SIR the process for protecting bystanders' identities when sharing footage or images from KSCO's Arial Support Unit in response to a Public Records Request.

Management Response

Concur Do Not Concur

Estimated Date of Implementation: None Provided

Response: This issue is not unique to FLIR. We will work with OIG and ITD to ensure that our overall PDR policy protects the identities of bystanders, as appropriate. Currently we would simply apply the same privacy review as we do with all PDRs. Further, KCSO would be the primary responding agency for PDRs related to FLIR footage.

2. 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.

Management Response

Concur Do Not Concur

Estimated Date of Implementation: December 31, 2023

Proposed Implementation Plan: SPD will update Policy 6.060.10 to include FLIR video.

Non-Audit Statement

This review was not conducted under Generally Accepted Government Auditing Standards. However, OIG has reviewed the work of Critical Insight to provide reasonable assurance that evidence used in this review was sufficient and appropriate.