City of Seattle

2024 Surveillance Impact Report

Real-Time Crime Center

Seattle Police Department

Surveillance Impact Report ("SIR") overview

About the Surveillance Ordinance

The Seattle City Council passed Ordinance 125376, also referred to as the "Surveillance Ordinance," on September 1, 2017. SMC 14.18.020.b.1 charges the City's executive with developing a process to identify surveillance technologies subject to the ordinance. Seattle IT, on behalf of the executive, developed and implemented a process through which a privacy and surveillance review is completed prior to the acquisition of new technologies. This requirement, and the criteria used in the review process, are documented in Seattle IT Policy PR-02, the "Surveillance Policy".

How this Document is Completed

This document is completed by the requesting department staff, support and coordinated by the Seattle Information Technology Department ("Seattle IT"). As Seattle IT and department staff complete the document, they should keep the following in mind.

1. Responses to questions should be in the text or check boxes only; all other information (questions, descriptions, etc.) Should **not** be edited by the department staff completing this document.

2. All content in this report will be available externally to the public. With this in mind, avoid using acronyms, slang, or other terms which may not be well-known to external audiences. Additionally, responses should be written using principally non-technical language to ensure they are accessible to audiences unfamiliar with the topic.

Surveillance Ordinance Review Process

The following is a high-level outline of the complete SIR review process.

Upcoming for Review	Initial Draft	Open Comment Period	Final Draft	Working Group	Council Review
The technology is upcoming for review, but the department has not begun drafting the surveillance impact report (SIR).	Work on the initial draft of the SIR is currently underway.	The initial draft of the SIR and supporting materials have been released for public review and comment. During this time, one or more public meetings will take place to solicit feedback.	During this stage the SIR, including collection of all public comments related to the specific technology, is being compiled and finalized.	The surveillance advisory working group will review each SIR's final draft and complete a civil liberties and privacy assessment, which will then be included with the	City Council will decide on the use of the surveillance technology, by full Council vote.

				SIR and submitted to Council.	

Privacy Impact Assessment

Purpose

A Privacy Impact Assessment ("PIA") is a method for collecting and documenting detailed information collected in order to conduct an in-depth privacy review of a program or project. A PIA asks questions about the collection, use, sharing, security and access controls for data that is gathered using a technology or program. It also requests information about policies, training and documentation that govern use of the technology. The PIA responses are used to determine privacy risks associated with a project and mitigations that may reduce some or all of those risks. In the interests of transparency about data collection and management, the City of Seattle has committed to publishing all PIAs on an outward facing website for public access.

When is a Privacy Impact Assessment Required?

A PIA may be required in two circumstances.

1. When a project, technology, or other review has been flagged as having a high privacy risk.
2. When a technology is required to complete the surveillance impact report process. This is one deliverable that comprises the report.

1.0 Abstract

1.1 Please provide a brief description (one paragraph) of the purpose and proposed use of the project/technology.

Real-Time Crime Center (RTCC) software provides a centralized location for real-time information and analysis. At its core, RTCC software integrates dispatch, camera, officer location, gunshot detection, 911 calls, records management systems, and other information into one "pane of glass" (a single view). The software is used to alert RTCC staff to a serious criminal event, see multiple streams of information overlaid on a map view, and convey information to officers responding in the field.

The purpose of RTCC software is to provide situational awareness to increase officer and community safety and reactively investigate incidents. Having real-time, accurate information in one place helps increase reliability regarding the location of victims and suspects – enabling quicker aid and safer apprehension. Having better visual and spatial suspect information helps reduce unnecessary stops by officers, focusing their efforts on verified locations and accurate descriptions.

1.2 Explain the reason the project/technology is being created or updated and why the PIA is required.

The Seattle Police Department (SPD) is currently experiencing unprecedented staffing shortages. Patrol officers are overwhelmed with calls for service, resulting in long wait times for lower-level calls. Investigators are fielding large caseloads, creating backlogs. RTCC software can help provide richer, more accurate information to resources in the field and investigations, helping more efficiently manage time spent on lengthy, serious crimes. In addition, increasing case clearance rates for investigators will lead to decreased crime rates and an increased responsiveness to victims of crime.

Real-time crime center software brings several technologies deemed surveillance technologies (CCTV, AGLS, ALPR, etc.) into one platform. In addition, some RTCC software uses non-generative AI, such as object detection, to analyze those surveillance technologies. Finally, the software stores information from these technologies either in the cloud or on-premise, creating some risks around data security and retention. Due to these factors, the City of Seattle Privacy Office has deemed the technology surveillance technology, which triggered this review.

2.0 Project / Technology Overview

Provide an overview of the project or technology. The overview gives the context and background necessary to understand the purpose, mission and justification for the project / technology proposed.

2.1 Describe the benefits of the project/technology.

As mentioned in previous responses, RTCC software can help mitigate staffing shortages for both patrol officers and investigations detectives by providing more reliable and accurate data on incidents in real-time.

Here is one example of how SPD might use the RTCC software to more efficiently utilize separate data sources to aid victims, capture dangerous suspects, and help remove firearms from the streets:

> A RTCC officer receives an alert through the RTCC software that there are gunshots on Aurora Avenue North. The software shows a map of the area on her monitor, with the associated dispatch call superimposed on the screen. The map shows the number and locations of the gunshots. Her map screen also automatically shows the feeds of the closest three CCTV cameras, as well as nearby patrol car locations. The officer sees on the RTCC map that the shots were fired on Aurora Avenue with successive gunshots moving in a northerly direction, most likely indicating that the shots were fired from a vehicle. She uses the RTCC software to enlarge the feed for the cameras north of the incident and sees a black Honda Civic moving at a high rate of speed in a northerly direction on Aurora.
>
> Using the software, she quickly pulls up the camera recording where the gunshots were fired and visually ascertains that the shots were fired from a black Honda and that there is a person down on the ground. She advises over SPD radio that there is a possible gunshot victim and gives a description of the Honda and the license plate. She sees from the software live camera feeds that the Honda is turning west on 125th Street, and that there is a patrol vehicle on that street 10 blocks west of Aurora and one 15 blocks south of the scene on Aurora. She advises over the radio that the suspect is heading west on 125th St. She goes back to the software live camera view

and surveys the shooting scene. The person is still down. No one else is at the scene. She relays via radio what she has seen through the RTCC software.

After the incident, she uses the RTCC software to create clips of all scenes showing the incident and the vehicle travel before, during and after the incident and uploads them from the RTCC software to the SPD digital evidence system.

At the same time this is happening, the officer driving north on Aurora gets dispatched to a possible shooting scene. The dispatcher informs her that there is a victim on the ground and the RTCC officer has observed no other people around the victim. The officer arrives on scene, exits her vehicle, takes a quick scan of the scene to confirm that the scene is secure. She grabs a first aid kit in her trunk, then runs to the victim on the ground and renders aid. In the background, she can hear the Fire Department sirens coming toward her. She radios dispatch and tells them the scene is secure for the arriving paramedics.

After the shooting scene is secure, a homicide detective arrives at the scene. Officers are using their flashlights and struggling to find bullet casings. The detective pulls up the RTCC application on his phone and brings up the information for the incident. He sees an overhead satellite map of the scene and notes how many shots were fired, the possible caliber of the weapon, and the approximate location of bullet evidence. He walks towards the officers and shows them the map – they move up the road a bit and eventually find as many casings as the software shows were fired. The detective listens to the audio on the phone app and can clearly hear five shots, evenly spaced – as many as the AGLS system said were fired. The detective then uses the software to view CCTV recordings of the incident, which has been shared with him on the application by the RTCC officer. He is satisfied there were no witnesses and proceeds with his work at the scene.

2.2 Provide any data or research demonstrating anticipated benefits.

Academic research related to the effect of real-time crime centers is limited; however, a 2023 John Jay College of Criminal Justice study showed that a real-time crime center in Chicago, IL increased case clearance rates 5% for violent crime, 12% for property crime, and 11% for overall crime. The authors conclude that “RTCCs may provide investigative benefits to police through the integration of technologies and data, thus enhancing case solvability.”

Other studies on the effects of technologies integrated with RTCC software, such as AGLS and CCTV, are discussed in their respective Surveillance Impact Reports.

2.3 Describe the technology involved.

The core of most RTCC software involves bringing in multiple sources of information into a single “pane of glass” (a single view). The sources of information that are being integrated with the software are current or expected SPD technologies such as the department's CAD system (computer-aided dispatch), acoustic gunshot location system (AGLS), closed-circuit television cameras (CCTV), automatic vehicle location (AVL) system, body and in-car video cameras, automated license plate readers (ALPR), digital evidence platforms, and 911 call systems.

Most of the technology comes into play around a mapping function which provides the overlay for all the other technologies. The mapping system includes roads, building layouts (when provided), and other layers like beat/sector boundaries. Most RTCC vendors provide this service via cloud-based web applications, as well as mobile applications for use in the field.

While most integrations between RTCC software and department applications occur between vendor APIs, some RTCC vendors use hardware for CCTV cameras that allow for the recording of the camera video, providing the ability to playback CCTV in the RTCC environment. RTCC software for CCTV cameras can also provide in-application video analytics that use machine-learned algorithms to analyze camera feeds and, using object recognition, locate specific items, people based on clothing, or vehicles based on description. This technology complies with the city of Seattle's AI rules for use, requiring a "human in the loop" at the initiation and evaluation of the results. SPD will not use facial recognition technology. In addition, SPD would not use analytics available in some platforms that combine different data sources and use algorithms or AI to present trends.

Some RTCC vendors produce hardware that allows for private camera owners (such as private businesses) to share specific camera feeds with agencies. This option would be fully voluntary at the discretion of the camera owners. Private camera owners can also set up conditional sharing, meaning they can determine the parameters of what, how, and when their camera feeds are shared. Some vendors also provide a registry so that private camera owners can share the location of the camera, but not the video feeds, so agencies can easily canvass for videos after an incident. The system can then allow SPD to send an email to all registered cameras in an area requesting relevant video. There is no obligation to share footage if a system is registered.

Some RTCC software vendors also include public-facing features such as notification software that allows an agency to push out real-time information to the public in the form of texts for those who opt-in. These functions are like Alert Seattle and Reverse 911 and could be used in large-scale events such as traffic re-routing or other disruptions.

There are also features that allow a rapid video response to calls for service. For example, a community member that calls 911 may be sent a link to their phone to opt-in to a video chat with a 911 operator or officer to provide face-to-face communication to help facilitate accurate officer response and/or medical aid instruction. The caller would need to opt-in to allow the use of their camera, microphone, and GPS. This service could be used in an active shooter situation to help officers assess the situation or other rapidly changing emergency environments.

Other potential features include tools that enable incident planning and real-time management across the department, including freehand sketching of maps, iconography, and roles-based viewing and editing access across a variety of connected devices. Fusing graphical illustration tools with live video and team geolocation creates a flexible and holistic view of emergent incidents, streamlining response capabilities. This feature would help incident commanders utilize mapping capabilities to better manage large-scale events.

Another potential feature allows officers to listen to 911 calls directly, helping to bring small details within the words, tone, or background that can aid responders in achieving desired outcomes. This type of feature would utilize 911 call recording already in use at the Seattle 911 call center.

Finally, some RTCC software systems have services that allow members of the public to anonymously submit multi-media tips by texting pictures, text, or video to a publicized number. Tips are then stored in the system for examination and potentially used as evidence.

2.4 Describe how the project or use of technology relates to the department's mission.

The mission of the SPD is to prevent crime, enforce the law, and support quality public safety by delivering respectful, equitable, professional, and dependable police services. SPD's department priorities include the use of best practices that include officer safety guidelines and performance-based accountability to provide progressive and responsive police services to crime victims, witnesses, and all members of the community and to structure the organization to support the SPD mission and field a well-trained sworn and non-sworn workforce that uses technology, training, equipment, and research strategically and effectively.

The RTCC software helps provide responsive police services to victims, witnesses, and members of the community by providing responders with more accurate and robust information that does not require significant staffing additions. Using technology that enables quicker and richer police response aligns with the SPD mission and will benefit the community as a whole.

2.5 Who will be involved with the deployment and use of the project / technology?

At the time of writing, planning is still underway for exactly who would use the RTCC software. The vision is for SPD to staff a real-time crime center with a combination of sworn officers and civilian staff, eventually transitioning to a more civilian-staffed model. Due to the wide functionality of RTCC software, it is likely incident commanders will use the software, as will some officers as safety, policy, and time allow.

The Office of the Inspector General will have full access to the RTCC operation.

3.0 Use Governance

Provide an outline of any rules that will govern the use of the project / technology. Please note: non-City entities contracting with the City are bound by restrictions specified in the surveillance ordinance and privacy principles and must provide written procedures for how the entity will comply with any restrictions identified.

3.1 Describe the processes that are required prior to each use, or access to/ of the project / technology, such as a notification, or check-in, check-out of equipment.

The RTCC will have a set of access controls based on what is required for each user. Only authorized/trained SPD and OIG personnel will have direct access. Data and information obtained through the RTCC may only be accessed or extracted for legitimate law enforcement purposes, as governed by SPD Policy 12.050.

3.2 List the legal standards or conditions, if any, that must be met before the project / technology is used.

The SPD does not currently have any policies related to RTCC. As RTCC will be the platform for different technologies such as CCTV and AGLS, any audio recordings or video that is captured will only be preserved as evidence if it is determined a crime has been committed.

The use of CCTV will comply with SMC Chapter 14.12, Collection of Information for Law Enforcement Purposes. All existing SPD policies related to technology and Criminal Justice Information Systems will apply to the RTCC. (Policy 12.050). All use of the RTCC will be for legitimate law enforcement purposes only and personal or inappropriate use or dissemination of information can result in internal discipline, termination, and penalties under federal or state law.

3.3 Describe the policies and training required of all personnel operating the project / technology, and who has access to ensure compliance with use and management policies.

Supervisors and commanding officers are responsible for ensuring compliance with SPD policies.

Access to the RTCC will only be made accessible to authorized SPD, OPA, and OIG personnel. Authorized personnel will receive training in the use of the RTCC management system prior to authorization.

All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), and any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.

4.0 Data Collection and Use

4.1 Provide details about what information is being collected from sources other than an individual, including other IT systems, systems of record, commercial data aggregators, publicly available data and/or other City departments.

The RTCC software integrates data from other SPD systems into a centralized location for real-time information and analysis. Data feeding into RTCC could come from dispatch, CCTVs, officer location, gunshot detection, 911 calls, records management systems (RMS), ALPR, geographic information systems (GIS), and other information systems. Information from some of these systems may be stored in storage related to the RTCC software to provide a comprehensive record of an incident.

SPD Policy 7.010 governs the submission of evidence and requires that all collected evidence be documented in a General Offense (GO) Report. Evidence is submitted to the Evidence Unit and associated with a specific GO Number and investigation.

4.2 What measures are in place to minimize inadvertent or improper collection of data?

The RTCC software is used to integrate existing data sources for which SPD already has access to into one piece of software. Those existing data sources have their own pre-existing controls in place to minimize inadvertent or improper collection, as outlined in previous surveillance impact reports for the relevant technology.

The RTCC software itself will store some of the data from the integrated systems to provide a comprehensive picture of an incident. Data that is not part of a criminal investigation will be subject to a 30-day retention policy, after which it will be purged from the system.

4.3 How and when will the project / technology be deployed or used? By whom? Who will determine when the project / technology is deployed and used?

The desired deployment date is mid-2024. SPD's vision is to have a RTCC staffed by a combination of sworn and civilian staff that will monitor the RTCC software and provide information to patrol officers and detectives. Access may be given to detectives and patrol officers in certain situations. The system will be used by incident commanders at the scenes of major crimes and events.

The SPD Technology and Innovation Unit will be the initial owner of the system and will manage implementation.

4.4 How often will the technology be in operation?

The technology will be in continuous operation.

4.5 What is the permanence of the installation? Is it installed permanently, or temporarily?

Installation of the RTCC software is permanent and will operate 24/7.

4.6 Is a physical object collecting data or images visible to the public? What are the markings to indicate that it is in use? What signage is used to determine department ownership and contact information?

There will be no new physical objects or sensors collecting data as part of the RTCC software package. It integrates existing data sources into one centralized platform.

4.7 How will data that is collected be accessed and by whom?

Only authorized SPD and OIG users can access the RTCC software platform. Access to the systems/technology is limited to authorized personnel via password-protected login credentials or single-sign on access.

Data extracted from the system/technology and entered into investigative files is securely inputted and used on SPD's password-protected network with access limited to authorized detectives and identified supervisory personnel.

All SPD employees are backgrounded and access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including SPD Policy 12.040 - Department-Owned Computers, Devices & Software, SPD Policy 12.050 - Criminal Justice Information Systems, SPD Policy 12.080 – Department Records Access, Inspection & Dissemination, SPD Policy 12.110 – Use of Department E-mail & Internet Systems, and SPD Policy 12.111 – Use of Cloud Storage Services.

All use of the RTCC will be for legitimate law enforcement purposes only. Personal or inappropriate use or dissemination of information can result in internal discipline, termination, and penalties under federal or state law.

4.8 If operated or used by another entity on behalf of the City, provide details about access, and applicable protocols.

Other law enforcement agencies have used similar RTCC platforms to share information during serious incidents that span jurisdictions. For example, an active shooter in the City of Atlanta was apprehended in a neighboring county that was using the same RTCC platform.

Any direct usage by a different jurisdiction will be consistent with SPD policy.

4.9 What are acceptable reasons for access to the equipment and/or data collected?

RTCC software will be accessed and used for serious incidents happening in real-time to provide information to patrol resources. It will also be used to provide a comprehensive picture of numerous SPD systems to investigators.

Data held in the RTCC system may only be viewed or extracted for legitimate law enforcement purposes, as governed by SPD Policy 12.050.

4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

RTCC software data will be stored within secure City of Seattle facilities under the administration of the Seattle Information Technology Department. If cloud storage is utilized, it will follow city security guidelines and only be accessible to outside parties as part of system maintenance and support only when authorized.

Various measures will be in place to protect data from unauthorized access.

- Data Encryption
- Access control mechanisms (*meeting CJIS requirements)
- Strict user permission settings
- Industry standard network security measures (meeting CJIS requirements)

The system will maintain audit logs of user and system actions. These logs will be maintained within the system and be accessible to those with permission to view. Logs will be accessible to the Office of Inspector General upon request.

* Criminal Justice Information Services (CJIS) Division of the Federal Bureau of Investigation (FBI) sets requirements for organizations that access or use criminal justice information. These requirements are referred to as "CJIS requirements" and are developed and audited for compliance by the FBI.

5.0 Data Storage, Retention and Deletion

5.1 How will data be securely stored?

Any incident or multimedia data extracted from the system will be stored in a method compliant with the FBI's CJIS requirements. The specific details are vendor dependent, but could include either cloud storage or on-premise storage.

5.2 How will the owner allow for departmental and other entities, to audit for compliance with legal deletion requirements?

Retention period for data stored in RTCC software storage will be 30 days and overwritten after that retention period expires. Data associated with criminal investigations will get saved as evidence and fall under retention guidelines for evidence.

Audits from the OIG or other official auditors, will be allowed as needed.

5.3 What measures will be used to destroy improperly collected data?

Per SIR section 5.2, RTCC data stored by the city will be automatically purged by the system after 30 days for any data that is not determined to be related to criminal activity/investigation.

SPD Policy 7.010 governs the submission of evidence and requires that all collected evidence be documented in a General Offense Report. Evidence is submitted to the Evidence Unit and associated with a specific GO Number and investigation.

All information must be gathered and recorded in a manner that is consistent with SPD Policy 6.060, such that it does not reasonably infringe upon "individual rights, liberties, and freedoms secured by the Constitution of the United States and of the State of Washington, including, among others, the freedom of speech, press, association and assembly; liberty of conscience; the exercise of religion; and the right to petition government for redress of grievances; or violate an individual's right to privacy."

All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), and any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.

5.4 which specific departmental unit or individual is responsible for ensuring compliance with data retention requirements?

Unit supervisors are responsible for ensuring compliance with data retention requirements within SPD.

Additionally, any appropriate auditor, including the OIG, can audit for compliance at any time.

6.0 Data Sharing and Accuracy

6.1 Which entity or entities inside and external to the City will be data sharing partners?

Data obtained from the technology may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law.

Data may be shared with outside entities in connection with criminal prosecutions:

- 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

Data may be made available to requesters pursuant to the Washington Public Records Act, Chapter 42.56 RCW ("PRA"). SPD will apply applicable exemptions to the data before disclosing to a requester. Individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.

Per SPD Policy 12.080, the Crime Records Unit is responsible for receiving, recording, and responding to requests “for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies.”

Discrete pieces of data collected or compiled by the RTCC software may be shared with other law enforcement agencies in wanted bulletins, and in connection with law enforcement investigations jointly conducted with those agencies, or in response to requests from law enforcement agencies investigating criminal activity as governed by SPD Policy 12.050 and 12.110. All requests for data from Federal Immigration and Customs Enforcement (ICE) authorities are referred to the Mayor’s Office Legal Counsel in accordance with the Mayoral Directive, dated February 6, 2018.

SPD shares data with authorized researchers pursuant to properly execute research and confidentiality agreements as provided by SPD Policy 12.055. This sharing may include discrete pieces of data related to specific investigative files collected by the devices.

6.2 Why is data sharing necessary?

Data sharing is necessary for SPD to fulfill its mission of contributing to crime reduction by assisting in collecting evidence related to criminal activity as part of investigations, and to comply with legal requirements.

6.3 Are there any restrictions on non-City data use?

Yes ☒ No ☐

6.3.1 If you answered yes, provide a copy of the department’s procedures and policies for ensuring compliance with these restrictions.

Law enforcement agencies receiving criminal history information are subject to the requirements of CFR Title 28, Part 20, regulating criminal justice information systems In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260 (auditing and dissemination of criminal history record information systems), and RCW Chapter 10.97 (Washington State Criminal Records Privacy Act).

Once disclosed in response to PRA request, there are no restrictions on non-City data use; however, applicable exemptions will be applied prior to disclosure to any requestor who is not authorized to receive exempt content.

6.4 How does the project/technology review and approve information sharing agreements, memorandums of understanding, new uses of the information, new access to the system by organizations within City of Seattle and outside agencies?

Sharing agreements must meet the standards reflected in SPD Policy 12.055. Law enforcement agencies receiving criminal history information are subject to the requirements of CFR Title 28, Part 20. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260, and RCW Chapter 10.97.

Following Council approval of the SIR, SPD must seek Council approval for any material change to the purpose or manner in which the RTCC software platform may be used.

6.5 Explain how the project/technology checks the accuracy of the information collected. If accuracy is not checked, please explain why.

Real-time crime center software data comes from various SPD systems and is blended into one single view/location. Accuracy of data flows over APIs are checked at the point of development and monitored by system administrator and system logging thereafter. The system administrator is responsible for monitoring API versioning and change management to proactively plan and avoid issues.

6.6 Describe any procedures that allow individuals to access their information and correct inaccurate or erroneous information.

Individuals may request records pursuant to the PRA, and individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.

7.0 Legal Obligations, Risks and Compliance

7.1 What specific legal authorities and/or agreements permit and define the collection of information by the project/technology?

Both the content and means of collection of information that may be utilized by the RTCC is regulated by the Fourth Amendment of the United States Constitution, Article I, Sec. 7 of the Washington State Constitution, case law interpreting the same, Washington's Privacy Act, RCW 9.73, CFR Title 28, Part 23, and Seattle's Intelligence Ordinance, SMC Chapter 14.12.

7.2 Describe what privacy training is provided to users either generally or specifically relevant to the project/technology.

SPD Policy 12.050 mandates that all SPD employees receive Security Awareness Training (Level 2), and all employees also receive City Privacy Training.

7.3 Given the specific data elements collected, describe the privacy risks identified and for each risk, explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

SMC 14.12 and SPD Policy 6.060 direct all SPD personnel to "any documentation of information concerning a person's sexual preferences or practices, or their political or religious activities must be for a relevant reason and serve a legitimate law enforcement purpose."

Additionally, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

7.4 Is there any aspect of the project/technology that might cause concern by giving the appearance to the public of privacy intrusion or misuse of personal information?

As stated above, RTCC software integrates dispatch, camera, officer location, gunshot detection, 911 calls, records management system, and other information into one platform. With the nature of data obtained through the RTCC, there is some risk that private information may be obtained about members of the public without their knowledge. This risk and those privacy risks outlined in 7.3 above are mitigated by legal requirements and auditing processes that allow for any auditor, including the Office of Inspector General, to inspect use and deployment of the RTCC software.

8.0 Monitoring and Enforcement

8.1 Describe how the project/technology maintains a record of any disclosures outside of the department.

Sharing of digital evidence outside the department is primarily done through SPD's digital evidence management system. Records of when data was shared and who it is shared with is noted in the system audit logs. Digital evidence shared outside of the digital evidence management system (e.g., using media such as DVDs, thumb drives, etc.) is done though SPD's Digital Forensic Unit, which logs requests.

Per SPD Policy 12.080, the Crime Records Unit is responsible to receive and record all requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies."

Any requests for public disclosure are logged by SPD's Public Disclosure Unit. Any action taken, and data released subsequently, is then tracked through the request log. Responses to Public Disclosure Requests, including responsive records provided to a requestor, are retained by SPD for two years after the request is completed.

8.2 What auditing measures are in place to safeguard the information, and policies that pertain to them, as well as who has access to the audit data? Explain whether the project/technology conducts self-audits, third party audits or reviews.

The Office of Inspector General conducts independent audits of SPD as instructed by the City Council and by City ordinance.

Financial Information

Purpose

This section provides a description of the fiscal impact of the surveillance technology, as required by the surveillance ordinance.

1.0 Fiscal Impact

Provide a description of the fiscal impact of the project/technology by answering the questions below.

1.1 Current or potential sources of funding: initial acquisition costs.

Current ☐ potential ☒

Date of initial acquisition	Date of go live	Direct initial acquisition cost	Professional services for acquisition	Other acquisition costs	Initial acquisition funding source
Q2 2024	Q3 2024	TBD	TBD	TBD	General Fund

Notes:

The SPD’s 2024 budget includes $1.5 million for the use of AGLS/CCTV/ALPR technologies. Since RTCC software integrates these technologies into one single “pane of glass” for effective use, SPD will use a portion of these funds for acquisition of the technology. At the time of writing, the procurement process has not yet been undertaken, so a breakdown of that funding has not yet happened.

1.2 Current or potential sources of funding: on-going operating costs, including maintenance, licensing, personnel, legal/compliance use auditing, data retention and security costs.

Current ☐ potential ☒

Annual maintenance and licensing	Legal/compliance, audit, data retention and other security costs	Department overhead	IT overhead	Annual funding source
TBD	TBD	TBD	TBD	TBD

Notes:

At the time of writing, the planning process has not yet been completed.

1.3 Cost savings potential through use of the technology

The use of RTCC software may help alleviate SPD’s shortage of sworn staffing by more effectively deploying patrol resources to incidents. While these objectives need to be evaluated, they do not necessarily correlate to direct cost savings, but may result in mitigating staffing shortages.

1.4 Current or potential sources of funding including subsidies or free products offered by vendors or governmental entities

No funding beyond city General Fund dollars have been identified for this technology.

Expertise and References

Purpose

The following information is provided to ensure that Council has a group of experts to reference while reviewing the completed surveillance impact report ("SIR"). Any individuals or agencies referenced must be made aware ahead of publication that their information has been included. All materials must be available for Council to access or review, without requiring additional purchase or contract.

1.0 Other Government References

Please list any other government bodies that have implemented this technology and can speak to the implementation of this technology.

Agency, municipality, etc.	Primary contact	Description of current use

2.0 Academics, Consultants, and Other Experts

Please list any experts in the technology under consideration, or in the technical completion of the service or function the technology is responsible for.

Agency, municipality, etc.	Primary contact	Description of current use

3.0 White Papers or Other Documents

Please list any publication, report or guide that is relevant to the use of this technology or this type of technology.

Title	Publication	Link
Bureau of Justice Assistance RTCC Information		https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/RealTimeCrimeCenterInformation.pdf

Racial Equity Toolkit (“RET”) and engagement for public comment worksheet

Purpose

Departments submitting a SIR are required to complete an adapted version of the Racial Equity Toolkit (“RET”) in order to:

- Provide a framework for the mindful completion of the SIR in a way that is sensitive to the historic exclusion of vulnerable and historically underrepresented communities. Particularly, to inform the public engagement efforts departments will complete as part of the surveillance impact report.
- Highlight and mitigate any impacts on racial equity from the adoption and the use of the technology.
- Highlight and mitigate any disparate impacts on individuals or vulnerable communities.
- Fulfill the public engagement requirements of the surveillance impact report.

Adaptation of the RET for Surveillance Impact Reports

The RET was adapted for the specific use by the Seattle Information Technology Departments’ (“Seattle IT”) Privacy Team, the Office of Civil Rights (“OCR”), and Change Team members from Seattle IT, Seattle City Light, Seattle Fire Department, Seattle Police Department, and Seattle Department of Transportation.

Racial Equity Toolkit Overview

The vision of the Seattle Race and Social Justice Initiative (“RSJI”) is to eliminate racial inequity in the community. To do this requires ending individual racism, institutional racism and structural racism. The RET lays out a process and a set of questions to guide the development, implementation and evaluation of policies, initiatives, programs, and budget issues to address the impacts on racial equity.

1.0 Set Outcomes

1.1. Seattle City Council has defined the following inclusion criteria in the surveillance ordinance, and they serve as important touchstones for the risks departments are being asked to resolve and/or mitigate. Which of the following inclusion criteria apply to this technology?

☐ The technology disparately impacts disadvantaged groups.

☐ There is a high likelihood that personally identifiable information will be shared with non-City entities that will use the data for a purpose other than providing the City with a contractually agreed-upon service.

☒ The technology collects data that is personally identifiable even if obscured, de-identified, or anonymized after collection.

☒ The technology raises reasonable concerns about impacts to civil liberty, freedom of speech or association, racial equity, or social justice.

1.2 What are the potential impacts on civil liberties through the implementation of this technology? How is the department mitigating these risks?

The technology will be used for the following purposes:

- Closed-Circuit (CCTV) camera systems will assist investigators in collecting evidence related to serious and violent crimes, including homicides, assaults, and other offenses. The CCTV system can aid investigators in identifying suspects, clearing the innocent, and removing deadly weapons from the street, thereby reducing the risk of harm to the public.
- The Acoustic Gunshot Location System (AGLS) will assist investigators in collecting evidence related to gunfire incidents and provide precise location information to responders. This information will direct officers and EMTs to a more precise location, enhance the collection of evidence that helps lead to justice for victims and remove illegal firearms from the community.
- Real-Time Crime Center (RTCC) software helps provide situational awareness to increase officers' and the public's safety and reactively investigate incidents. Having real-time, accurate information in one place helps increase the reliability of the location of victims and suspects, enabling quicker aid and safer apprehension. Having better visual and spatial suspect information will help reduce unnecessary stops by officers, focusing their efforts on verified locations and accurate descriptions.

Potential impacts on civil liberties include but are not limited to:

- Privacy concerns associated with surveillance of people, vehicles, and license plates in public places.
- Misuse of collected video and information/mission creep.
- Lack of transparency with the public on what is being done with recordings.
- Loss of personal autonomy with surveillance of an area.

To mitigate these potential community concerns, SPD will:

- Post signs indicating that police surveillance and video recordings are occurring.
- Ensure technology is being used for crimes related to gun violence, human trafficking, and other persistent crimes in the surveillance area.
- SPD will create a public-facing dashboard that will update frequently and report on the uses of the technologies, including areas where cameras are recording, mapping of where AGLS alerts are coming from, and the resulting number of police actions, such as arrests, court-authorized warrants, recovery of stolen vehicles, or other law enforcement actions.
- CCTV technology will only monitor public places, such as sidewalks, streets, and parks.
- Recorded material will only be kept for 30 days unless it is evidence of criminal behavior, in which case it will be transferred to SPD's secure digital evidence storage system.
- Provide access to CCTV, AGLS, ALPR, and SPD's Real Time Crime Center (RTCC) user and device logs to the Office of Inspector General (OIG) for compliance audits.
- The Office of the Inspector General will have full access to the RTCC operation.

Additionally, the technologies will only be implemented once the City's surveillance ordinance requirements are met and the City Council authorizes the use.

1.3 What are the risks for racial or ethnicity-based bias through each use or deployment of this technology? How is the department mitigating these risks?

Include a description of any issues that may arise such as algorithmic bias or the possibility for ethnic bias to emerge in people and/or system decision-making.

The mission of the Seattle Police Department is to prevent crime, enforce the law, and support quality public safety by delivering respectful, professional, and dependable police services. SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior and other accountability measures. This pilot will be data-informed and guided. It will terminate if data suggests the technology is ineffective. Utilizing the abilities of the Performance Analytics and Research Unit, the Seattle Police Department has a plan to actively manage performance measures reflecting the "total cost of ownership of public safety," Equity, Accountability, and Quality ("EAQ"), which includes measures of disparate impact and over policing. In addition to a robust *Continuous Intervention Assessment* designed to inform, in real-time, the active development of a safer and more effective, Evidence-Based Policing (EBP) competency, the EAQ program assures *just right* policing is achieved with undue collateral harm.

It's worth noting that many factors can contribute to disparate impacts in policing, most of which occur early in a person's life, long before there is engagement with the police. For example, systems and policies that perpetuate poverty, the failure to provide children with the strong and fair start they deserve in the crucial birth-to-five years, inadequate public education, and a lack of economic opportunity can all contribute to disparate outcomes. In addition, family dynamics and peer pressure can also create negative outcomes. We recognize these factors and strive to do our part to mitigate them, but we can't expect our police officers by themselves to cure these contributory factors. However, we do expect our officers to do their jobs respectfully and fairly as they interact with community members.

These technologies are location-specific, with a place-based focus, meaning they will record people who choose to be in a public place where the technologies are being used. This mitigating factor reduces, to an extent, the possible disparate impact of potential police actions.

1.4 Where in the City is the technology used or deployed?

The following neighborhoods are being considered for deploying the CCTV and AGLS technologies. Specific areas will be selected based on the data analysis indicating where gun violence, human trafficking, and persistent felony crimes are concentrated.

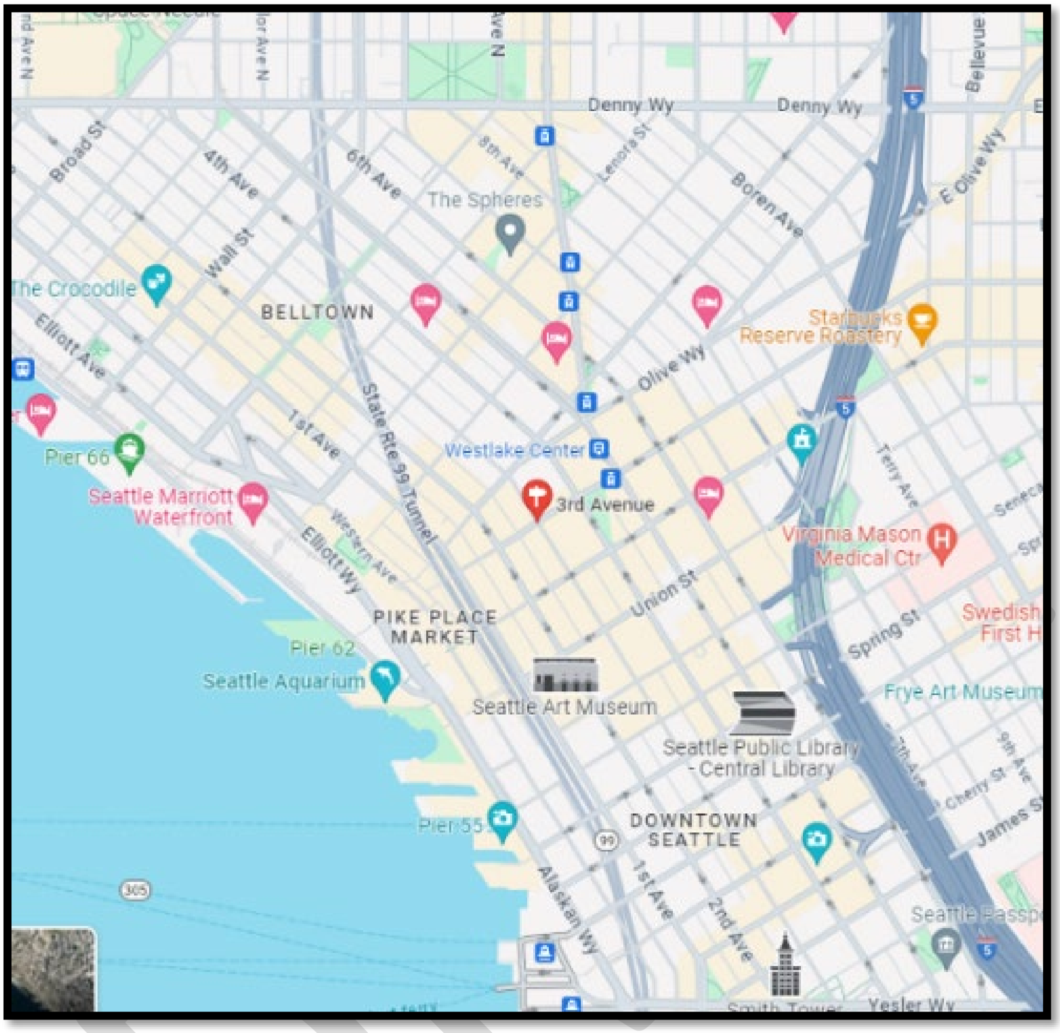
☐ all Seattle neighborhoods

☒ **Aurora Ave N 85th to 145th**
☐ Ballard
☒ **Belltown**
☐ Beacon Hill
☐ Capitol Hill
☐ Central District
☒ **Chinatown/International District**
☐ Columbia City
☒ **Downtown Commercial Core**
☐ Delridge
☐ First Hill
☐ Georgetown
☐ Greenwood / Phinney
☐ International District
☐ Interbay
☐ North
☐ Northeast

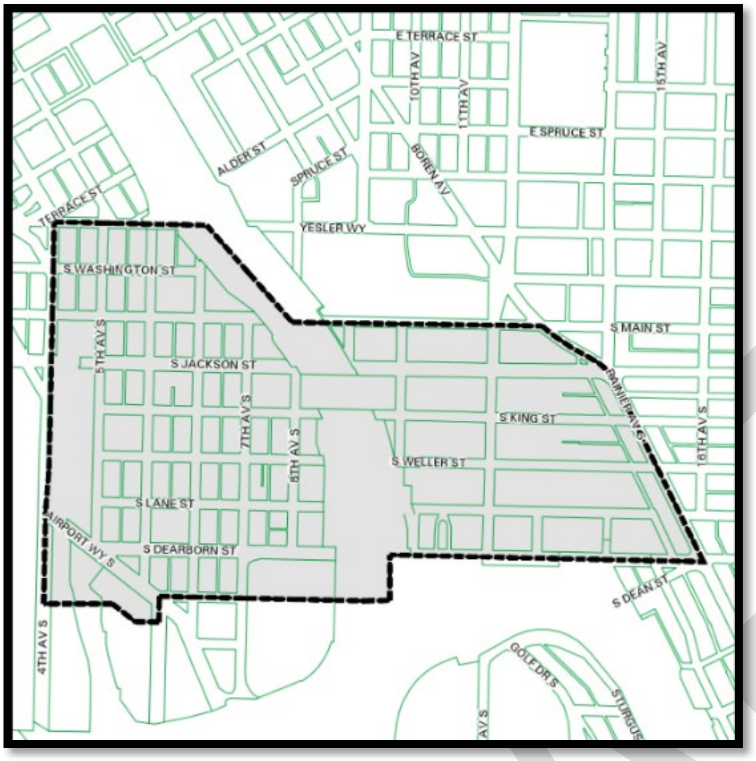
☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☐ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake
☐ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle) (Mutual Aid)
☐ Outside King County (Mutual Aid)

If possible, please include any maps or visualizations of historical deployments / use.

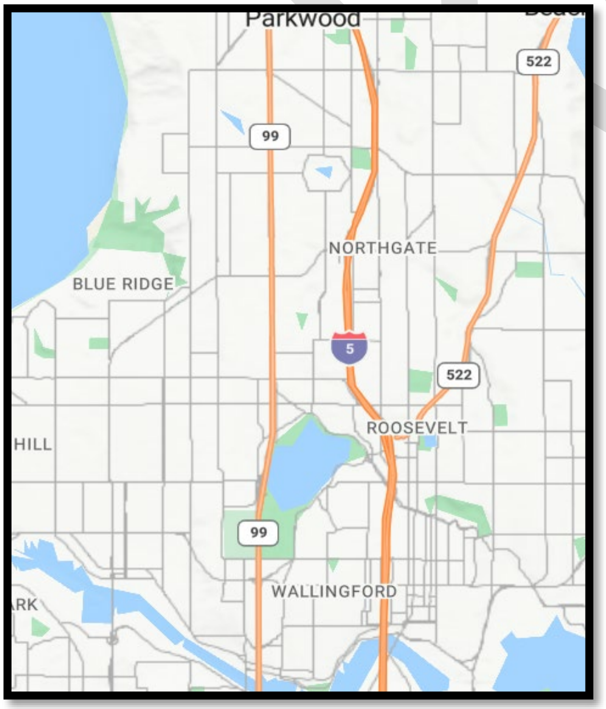
Downtown & Belltown Area



Chinatown-International District Area



Aurora Avenue North Corridor



1.4.1 What are the racial demographics of those living in this area or impacted by these issues?

Race/Ethnicity	Aurora	Chinatown International District	Belltown	Downtown Commercial	Citywide
American Indian or Alaska Native	0.8%	0.7%	0.6%	1.1%	0.4%
Asian	14.0%	49.2%	30.4%	16.8%	16.9%
Black/African American	8.9%	8.6%	5.5%	11.1%	6.8%
Hispanic or Latino of Any Race	11.3%	7.6%	7.1%	8.3%	8.2%
Native Hawaiian or Pacific Islander	0.3%	0.2%	0.2%	0.3%	0.3%
Other	0.7%	0.7%	0.6%	0.7%	0.6%
Multiple Races	7.9%	5.8%	4.9%	5.6%	7.3%
White	56.2%	27.2%	50.8%	56.1%	59.5%

Source: U.S. Census Bureau Decennial Census; OPCD

Note: Geographical areas provided are 2020 Census Block Assignments of Urban Villages within the Downtown Urban Center, with the exception of Aurora. Aurora's boundaries are based on ½ mile buffer from Aurora between Meridian and Greenwood, and from 85th to 145th.

1.4.2 How does the Department to ensure diverse neighborhoods, communities, or individuals are not specifically targeted through the use or deployment of this technology?

The use of CCTVs and AGLS will be deployed where crimes related to gun violence, human trafficking, and other persistent felony crimes are concentrated. SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as other accountability measures. This technology does not enhance the risks of racial or ethnicity-based bias.

These technologies are geographically focused on specific areas where gun violence, human trafficking, and other persistent felony crimes are concentrated. They are focused on individuals only if they are present in these areas.

1.5 How do decisions around data sharing have the potential for disparate impact on historically targeted communities? What is the department doing to mitigate those risks?

Data from the technology may be shared outside SPD with other agencies, entities, or individuals within legal guidelines or as required by law. Data may be shared with outside entities in connection with criminal prosecutions.

Data may be made available to requesters under the Washington Public Records Act, Chapter 42.56 RCW (“PRA”).

Data sharing has the potential to be a contributing factor to disparate impact on historically marginalized communities. To mitigate this possibility, SPD has established policies regarding disseminating data related to criminal prosecutions, Washington Public Records Act (Chapter 42.56 RCW), and authorized researchers. Further, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior.

1.6 How do decisions around data storage and retention have the potential for disparate impact on historically targeted communities? What is the department doing to mitigate those risks?

As with decisions around data sharing, data storage and data retention have similar potential for disparate impact on historically marginalized communities. The use of CCTVs and AGLS will be deployed where crimes related to gun violence, human trafficking, and other persistent felony crimes are concentrated. Video from CCTVs will be stored for 30 days unless imagery is needed for investigations or to comply with legal requirements. Further, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, and other accountability measures.

1.7 What are potential unintended consequences (both negative and positive potential impact)? What proactive steps can you can / have you taken to ensure these consequences do not occur.

The most important unintended possible negative consequence related to the implementation of CCTVs and AGLS is the possibility that the civil rights of individuals may be compromised by unreasonable surveillance. To mitigate this risk, SPD is enacting a specific policy codifying the allowable circumstances under which SPD may utilize CCTVs, AGLS, and Real-Time Crime Center software. Access to user and device logs will be given to the OIG so they can audit the use of these technologies.

To prevent unintended outcomes, the City will develop signage in areas that are covered by the cameras' view to alert the public to their presence and use. Additionally, the Office of the Inspector General will have access at any time to monitor and evaluate the use of these technologies. During the public outreach sessions described below, the City will listen to feedback from the public and provide responses during the technology review process.

The potential positive impact will be reduced serious crime concentrated in the locations where the technologies are deployed. If achieved, these reductions will create a safer environment for everyone who lives, works, plays, or visits these areas.

2.0 Public Outreach

2.1 Organizations who received a personal invitation to participate.

Please include a list of all organizations specifically invited to provide feedback on this technology.

The list of organizations will be listed in the final SIR.

2.1 Scheduled public meeting(s).

Meeting notes, sign-in sheets, all comments received, and questions from the public will be included in Appendix B, C, D, E, F, G, H and I. Comment analysis will be summarized in section 3.0 Public Comment Analysis.

Location	**Webex virtual meeting and in person option at the Bertha Knight Landes Room located on Floor 1 of City Hall (600 Fourth Avenue, Seattle, WA 98104)**
Time	February 12, 2024, 12:00 pm

Location	**Webex virtual meeting and in person option at a Community Center (details will be posted online shortly).**
Time	February 27, 2024, 6:00 pm

3.0 Public Comment Analysis

This section will be completed after the public comment period has been completed on [DATE] by Privacy Office staff.

3.1 Summary of Response Volume

Dashboard of respondent demographics.

3.2 Question One: What concerns, if any, do you have about the use of this technology?

Dashboard of respondent demographics.

3.3 Question Two: What value, if any, do you see in the use of this technology?

Dashboard of respondent demographics.

3.4 Question Three: What would you want City leadership to consider when making a decision about the use of this technology?

Dashboard of respondent demographics.

3.5 Question Four: General response to the technology.

Dashboard of respondent demographics.

3.5 General Surveillance Comments

These are comments received that are not particular to any technology currently under review.

Dashboard of respondent demographics.

4.0 Response to Public Comments

This section will be completed after the public comment period has been completed on [DATE].

4.1 How will you address the concerns that have been identified by the public?

What program, policy and partnership strategies will you implement? What strategies address immediate impacts? Long-term impacts? What strategies address root causes of inequity listed above? How will you partner with stakeholders for long-term positive change?

5.0 Equity Annual Reporting

5.1 What metrics for this technology be reported to the CTO for the annual equity assessments?

The goals of this project are:

1. Reduction in gun violence, human trafficking, and other persistent felony crimes in the pilot area.
2. Reduction in 911 calls in the pilot area.
3. To minimize crime displacement outside of the pilot area.
4. Improved police response times, crime clearance rates, and community satisfaction measures.

We will also report the rate of arrests and prosecutions that occur as a result of the pilot and any negative unintended consequences, such as over or under policing.

The Seattle Police Department, utilizing the Data Analytics Team and working with the Office of the City Auditor, will monitor these objectives and the outcomes closely to watch for disparate impacts. If data analysis shows any disparate impacts, SPD will work with the Auditor and the Office of the Inspector General to make the needed changes to address these impacts.

Privacy and Civil Liberties Assessment

Purpose

This section shall be completed after public engagement has concluded and the department has completed the racial equity toolkit section above. The privacy and civil liberties assessment is completed by the community surveillance working group ("working group"), per the surveillance ordinance which states that the working group shall:

"Provide to the executive and the City Council a privacy and civil liberties impact assessment for each SIR that must be included with any departmental request for surveillance technology acquisition or in-use approval. The impact assessment shall include a description of the potential impact of the surveillance technology on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities. The CTO shall share with the working group a copy of the SIR that shall also be posted during the period of public engagement. At the conclusion of the public engagement period, the CTO shall share the final proposed SIR with the working group at least six weeks prior to submittal of the SIR to Council for approval. The working group shall provide its impact assessment in writing to the executive and the City Council for inclusion in the SIR within six weeks of receiving the final proposed SIR. If the working group does not provide the impact assessment before such time, the working group must ask for a two-week extension of time to City Council in writing.   If the working group fails to submit an impact statement within eight weeks of receiving the SIR, the department and City Council may proceed with ordinance approval without the impact statement."

Working Group Privacy and Civil Liberties Assessment

Respond here.

Submitting Department Response

Description

Provide the high-level description of the technology, including whether software or hardware, who uses it and where/when.

Purpose

State the reasons for the use cases for this technology; how it helps meet the departmental mission; benefits to personnel and the public; under what ordinance or law it is used/mandated or required; risks to mission or public if this technology were not available.

Benefits to the Public

Provide technology benefit information, including those that affect departmental personnel, members of the public and the City in general.

Privacy and Civil Liberties Considerations

Provide an overview of the privacy and civil liberties concerns that have been raised over the use or potential mis-use of the technology; include real and perceived concerns.

Summary

Provide summary of reasons for technology use; benefits; and privacy considerations and how we are incorporating those concerns into our operational plans.

Appendix A: Glossary

Accountable: (taken from the racial equity toolkit.) Responsive to the needs and concerns of those most impacted by the issues you are working on, particularly to communities of color and those historically underrepresented in the civic process.

Community outcomes: (taken from the racial equity toolkit.) The specific result you are seeking to achieve that advances racial equity.

Contracting equity: (taken from the racial equity toolkit.) Efforts to achieve equitable racial outcomes in the way the City spends resources, including goods and services, consultants and contracting.

DON: “department of neighborhoods.”

Immigrant and refugee access to services: (taken from the racial equity toolkit.) Government services and resources are easily available and understandable to all Seattle residents, including non-native English speakers. Full and active participation of immigrant and refugee communities exists in Seattle’s civic, economic and cultural life.

Inclusive outreach and public engagement: (taken from the racial equity toolkit.) Processes inclusive of people of diverse races, cultures, gender identities, sexual orientations and socio-economic status. Access to information, resources and civic processes so community members can effectively engage in the design and delivery of public services.

Individual racism: (taken from the racial equity toolkit.) Pre-judgment, bias, stereotypes about an individual or group based on race. The impacts of racism on individuals including white people internalizing privilege, and people of color internalizing oppression.

Institutional racism: (taken from the racial equity toolkit.) Organizational programs, policies or procedures that work to the benefit of white people and to the detriment of people of color, usually unintentionally or inadvertently.

OCR: “Office of Civil Rights.”

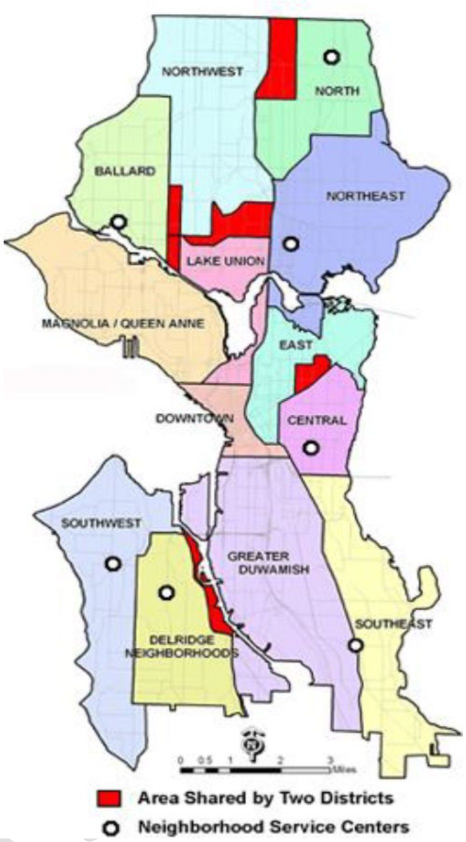
Opportunity areas: (taken from the racial equity toolkit.) One of seven issue areas the City of Seattle is working on in partnership with the community to eliminate racial disparities and create racial equity. They include: education, health, community development, criminal justice, jobs, housing, and the environment.

Racial equity: (taken from the racial equity toolkit.) When social, economic and political opportunities are not predicted based upon a person’s race.

Racial inequity: (taken from the racial equity toolkit.) When a person's race can predict their social, economic, and political opportunities and outcomes.

RET: "racial equity toolkit"

Seattle neighborhoods: (taken from the racial equity toolkit neighborhood.) Boundaries defined for the purpose of understanding geographic areas in Seattle.



Stakeholders: (taken from the racial equity toolkit.) Those impacted by proposed policy, program, or budget issue who have potential concerns or issue expertise. Examples might include: specific racial/ethnic groups, other institutions like Seattle housing authority, schools, community-based organizations, change teams, City employees, unions, etc.

Structural racism: (taken from the racial equity toolkit.) The interplay of policies, practices and programs of multiple institutions which leads to adverse outcomes and conditions for communities of color compared to white communities that occurs within the context of racialized historical and cultural conditions.

Surveillance ordinance: Seattle City Council passed ordinance 125376, also referred to as the "surveillance ordinance."

SIR: "surveillance impact report", a document which captures the fulfillment of the Council-defined surveillance technology review process, as required by ordinance 125376.

Workforce equity: (taken from the racial equity toolkit.) Ensure the City's workforce diversity reflects the diversity of Seattle.

Appendix B: Questions and Department Responses

Appendix C: Meeting Notice(s)

Appendix D: Additional Comments Received from Members of the Public *

Appendix E: Letters from Organizations or Commissions

Appendix F: Supporting Policy Documentation