POWERFUL TECHNOLOGY SOLUTIONS
FOR THE CITY AND PUBLIC WE SERVE

~~2018~~

2023 Surveillance Impact Report

~~AUTOMATED LICENSE PLATE RECOGNITION (ALPR) (PATROL)~~

~~SEATTLE POLICE DEPARTMENT~~

Style Definition: Normal: Font: 12 pt, Level 3, Space Before: 6 pt, After: 6 pt, Keep with next, Keep lines together

Style Definition: Heading 1: Font color: Auto, Not All caps, Space Before: 6 pt, After: 6 pt

Style Definition: Heading 2: Font: 14 pt, Font color: Custom Color(RGB(0,70,173)), Not All caps, Space Before: 6 pt, After: 6 pt, Keep lines together

Style Definition: Heading 3: Font: Not All caps, Space Before: 6 pt, After: 6 pt

Style Definition: Heading 4: Space Before: 6 pt

Style Definition: Heading 6: Font: 12 pt

Style Definition: Title: Font: Level 3, Space Before: 6 pt, Keep with next, Keep lines together

Style Definition: Subtitle: Font color: Custom Color(RGB(0,70,173)), Level 3, Space Before: 6 pt, After: 6 pt, Keep with next, Keep lines together

Style Definition: Table of Figures: Font: 12 pt, Level 3, Space Before: 6 pt, Keep with next, Keep lines together

Style Definition: TOC 1: Font: 14 pt, Font color: Custom Color(RGB(0,70,173)), Not All caps, Level 3, Keep with next, Keep lines together

Style Definition: Body Text 2: Font: 12 pt, Level 3, Space Before: 6 pt, Keep with next, Keep lines together

Style Definition: TOC 2: Font: 12 pt, Not All caps, Level 3, Space Before: 6 pt, Keep with next, Keep lines together

Style Definition: TOC 3: Not All caps, Level 3, Space Before: 6 pt, Keep with next, Keep lines together

Style Definition: Hyperlink: Font color: Custom Color(RGB(0,70,173))

Style Definition: Comment Text: Font: Level 3, Space Before: 6 pt, After: 6 pt, Keep with next, Keep lines together

Style Definition: Normal (Web): Font: 12 pt, Level 3, Keep with next, Keep lines together

Formatted: Font: 17 pt, Bold, Expanded by 0.75 pt

Formatted: No Spacing

03.16.2016

Seattle
Information Technology

~~Contents~~

City of Seattle

Formatted: Indent: Left: 0"

AUTOMATED LICENSE PLATE RECOGNITION (ALPR) (FLEET-WIDE)

Seattle Police Department

City of Seattle

Formatted: Indent: Left: 0"

Surveillance Impact Report ("SIR") overview

About the Surveillance Ordinance

Formatted: No Spacing, Space After: 6 pt, Line spacing: single

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 SIR and submitted to Council.	City Council will decide on the use of the surveillance technology, by full Council vote.

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.

Formatted: Indent: Left: 0"

1.0 Abstract

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

Seattle Police Department facilitates the flow of traffic (by monitoring and enforcing City parking restrictions) and recovers lost and stolen property through a number of means including Automated License Plate Reader (ALPR) technology. ALPR is utilized in recovery of lost or stolen property, to assist with active investigations, Scofflaw Law enforcement, and parking enforcement.

This Surveillance Impact Report focuses on SPD use of ALPR as a necessary law enforcement tool in two capacities:

1. Property Recovery – SPD employs ALPR to locate stolen vehicles (usually abandoned), as well as other vehicles subject to search warrant.
2. Investigation – On occasion, SPD relies on licenses plate reads to locate vehicle placement within the past 90 days (retention period), in the course of an active investigation or in support of legal proceedings.

Note that ALPR usage for parking enforcement is discussed in the Surveillance Impact Report entitled "Parking Enforcement Systems."

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

ALPR collects license plate information from vehicles, which could, if unregulated and indiscriminately used, be linked to other data to personally identify individuals.

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

Formatted: No Spacing

2.1 Describe the benefits of the project/technology.

The benefit of ALPR is many-fold. ALPR assists the City in managing flow of traffic (by monitoring and enforcing City parking restrictions) and locating and recovering lost/stolen property. Additionally, the ALPR system aids with active investigations by helping to determine the location of vehicles of interest – specifically those that have been identified as being associated with an investigation or disposition.

2.2 Provide any data or research demonstrating anticipated benefits.

General news reporting about ALPR Benefits: https://patch.com/california/glendora/plate-reader-helps-police-find-stolen-cars-make-warrant-arrests

Formatted: No Spacing, Space Before: 0 pt, After: 0 pt, Line spacing: single

Formatted: Indent: Left: 0"

2.3 Describe the technology involved.

~~ALPR hardware consists of high definition infrared digital cameras that are mounted on eight Patrol cars (one of which is unmarked).~~

~~The high-speed cameras capture images of license plates as they move into view, and associated software deciphers the characters on the plate, using optical character recognition. This interpretation is then immediately checked against any license plate numbers that have been uploaded into the onboard, in-vehicle software system. Twice a day, the License Plate Reader File (known as the HotList), a list of license plate numbers from Washington Crime Information Center (WACIC) and the FBI's National Crime Information Center (NCIS), is uploaded into the ALPR system (via a connection to WACIC), which is a source of "hits" for the license plate reader system. The license plate numbers compiled on the HotList "may be stolen vehicles, vehicles wanted in conjunction with felonies, wanted persons, and vehicles subject to seizure based on federal court orders" (WSP Memorandum of Understanding No. C141174GSC; March 11, 2014). Other sources include the City of Seattle Municipal Court's scofflaw list and content uploaded for over-time and metered parking enforcement (which are covered in the Parking Enforcement Systems SIR). No ALPR data collected by SPD are automatically uploaded into any system outside of SPD.~~

~~SPD contracts with Neology to provide both hardware and software for the PIPS ALPR system, used in Patrol. In addition to the cameras, Neology provides the backend server, known as BOSS, through which camera reads are interpreted and administrative control is managed. This includes the ability to set and verify retention periods, track and log user activity, view camera "read" and "hit" data, and manage user permissions.~~

~~The configuration is designed such that the cameras capture the images and filter the reads through the aforementioned linked software to determine if/when a hit occurs.~~

~~When the software identifies a hit, it issues an audible alert, and a visual notification informs the user which list the hit comes from – HotList; Scofflaw; time-restricted over time parking.~~

~~In ALPR-equipped Patrol vehicles, this triggers a chain of responses from the user that includes visual confirmation that the computer interpretation of the camera image is accurate, and the officer verbally checks with Dispatch for confirmation that the license plate is truly of interest before any action is taken. This is done to ensure the system accurately read a license plate. When an inaccuracy is detected, users may choose to enter a note into the system that the "hit" was a misread.~~

~~All data collected by the ALPR systems – images, computer-interpreted license plate numbers, date, time, and GPS location – are stored on-premises on a secure server within SPD and retained for 90 days. After 90 days, all data collected by the ALPR systems is automatically deleted (unless it has been flagged as serving an investigative purpose – in which case, it is included in an investigation file).~~

Formatted: Indent: Left: 0"

Fleet-wide ALPR for SPD Patrol operations is a component of the Axon Fleet 3 in-car video platform.

The high-speed cameras capture images of license plates as they move into view, and associated software deciphers the characters on the plate, using optical character recognition. This interpretation is then immediately checked against any license plate numbers that have been uploaded into the onboard, in-vehicle software system. Twice a day, the License Plate Reader File (known as the HotList), a list of license plate numbers from Washington Crime Information Center (WACIC) and the FBI's National Crime Information Center (NCIS), is uploaded into the ALPR system (via a connection to WACIC), which is a source of "hits" for the license plate reader system. The license plate numbers compiled on the HotList "may be stolen vehicles, vehicles wanted in conjunction with felonies, wanted persons, and vehicles subject to seizure based on federal court orders" (WSP Memorandum of Understanding No. C141174GSC; March 11, 2014). Other sources include the City of Seattle Municipal Court's scofflaw list and content uploaded for over-time and metered parking enforcement (which are covered in the Parking Enforcement Systems SIR). No ALPR data collected by SPD are automatically uploaded into any system outside of SPD.

SPD contracts with Axon to provide both ALPR enabled in-car video hardware and software for the Fleet 3 Hub software system through which camera reads are interpreted and administrative control is managed. This includes the ability to set and verify retention periods, track and log user activity, view camera "read" and "hit" data,~~,~~ and manage user permissions.

The configuration is designed such that the cameras capture the images and filter the reads through the linked Fleet 3 Hub software to determine if/when a hit occurs.

When the software identifies a hit, it issues an audible alert, and a visual notification informs the user which list the hit comes from – HotList; Scofflaw; time-restricted over time parking.

A "HIT" triggers a chain of responses from the user that includes visual confirmation that the computer interpretation of the camera image is accurate, and the officer verbally checks with Dispatch for confirmation that the license plate is truly of interest before any action is taken. This is done to ensure the system accurately read a license plate. When an inaccuracy is detected, users may choose to enter a note into the system that the "hit" was a misread.

All data collected by the ALPR systems – images, computer-interpreted license plate numbers, date, time, and GPS location – are stored and retained for 90 days. After 90 days, all data collected by the ALPR systems is automatically deleted (unless it has been flagged as serving an investigative purpose – in which case, it is included in an investigation file).

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

~~Seattle Police Department uses ALPR technology in its pursuit of maintaining public safety and enforcing applicable laws related to stolen vehicles and other crimes.~~

Formatted: Indent: Left: 0"

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'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.

Seattle Police Department uses ALPR technology in its pursuit of maintaining public safety and enforcing applicable laws related to stolen vehicles and other crimes.

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

~~As it relates to Patrol use, each precinct has the ability to utilize one or more of the vehicles at any time. Each precinct determines, based on its unique operational needs, for itself if/when/where it will deploy ALPR-equipped vehicles. Precincts work together to determine how to share the vehicles – dependent on their operational needs. Only sworn officers that have been trained in its use – carried out by another trained sworn officer and confirmed by the ALPR administrator – can sign out an ALPR-equipped vehicle in Patrol. Each precinct determines which officers will use the ALPR-equipped vehicles at which time, dependent on operational need.~~

~~The Technical and Electronic Support Unit (TESU), maintains administrative control of much of SPD's physical technology. The ALPR administrator is a member of TESU. The ALPR administrator monitors and manages user access to the PIPS ALPR system for Patrol. Housing management of the Patrol ALPR system in one unit makes oversight and accountability more efficient than tasking individual units or precincts with this themselves.~~

Formatted: Indent: Left: 0"

All SPD vehicles with onboard in-car video will have ALPR functionality enabled. All sworn SPD officers will be trained in the use of the in-car video with ALPR enabled functionality.

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.

Prior to gaining access to the ALPR system, potential users must be trained by other trained officers. Once this training has been verified with the ALPR administrator, users are given access and must log into the system with unique login and password information whenever they employ the technology. They remained logged into the system the entire time that the ALPR system is in operation. The login is logged and auditable.

Patrol Officers are assigned the vehicles to use while on-shift.

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

ALPR systems can be used during routine patrol or specific to a criminal investigation (i.e., to locate a stolen vehicle), as per SPD Policy 16.170.

The policy requires that users must be trained; they must be certified in A Central Computerized Enforcement Service System (ACCESS) – a computer controlled communications system maintained by Washington State Patrol that extracts data from multiple repositories, including Washington Crime Information Center, Washington State Identification System, the National Crime Information Center, the Department of Licensing, the Department of Corrections Offender File, the International Justice and Public Safety Network, and PARKS - and trained in the proper use of ALPR. In addition, the policy limits use of the technology to strictly routine patrol or criminal investigation. Further, the policy clarifies that users may only access ALPR data when that data relates to a specific criminal investigation. A record of these requests is maintained by the ALPR administrator.

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.

~~Include links to all policies referenced.~~

Formatted: Indent: Left: 0"

~~SPD Policy 16.170 addresses Automatic License Plate Readers. The policy requires that users must be trained; they must be certified in A Central Computerized Enforcement Service System (ACCESS) – a computer controlled communications system maintained by Washington State Patrol that extracts data from multiple repositories, including Washington Crime Information Center, Washington State Identification System, the National Crime Information Center, the Department of Licensing, the Department of Corrections Offender File, the International Justice and Public Safety Network, and PARKS - and trained in the proper use of ALPR. In addition, the policy limits use of the technology to strictly routine patrol or criminal investigation. Further, the policy clarifies that users may only access ALPR data when that data relates to a specific criminal investigation. A record of these requests is maintained by the ALPR administrator.~~

~~A member of TESU monitors compliance for ALPR use for Patrol.~~

Formatted: Indent: Left: 0"

SPD Policy 16.170 addresses Automatic License Plate Readers. The policy requires that users must be trained; they must be certified in A Central Computerized Enforcement Service System (ACCESS) – a computer controlled communications system maintained by Washington State Patrol that extracts data from multiple repositories, including Washington Crime Information Center, Washington State Identification System, the National Crime Information Center, the Department of Licensing, the Department of Corrections Offender File, the International Justice and Public Safety Network, and PARKS - and trained in the proper use of ALPR. In addition, the policy limits use of the technology to strictly routine patrol or criminal investigation. Further, the policy clarifies that users may only access ALPR data when that data relates to a specific criminal investigation. A record of these requests is maintained by the ALPR administrator.

SPD's Audit Unit monitors compliance for ALPR use for Patrol.

Formatted: Indent: Left: 0"

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.

Data collected from ALPR include license plate image, computer-interpreted read of the license plate number, date, time, and GPS location.

All ALPR-equipped vehicles upload a daily HotList that contains only license plate numbers, with the associated states, that are under active search warrant from NCIC and WASIC.

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

Formatted: Heading 3, Space After: 0 pt, Line spacing: single

When the ALPR system registers a hit – a match to license plate number listed on the HotList (as described in 2.3 above) - the user must verify accuracy before taking any action. For instance, when the system registers a hit on a stolen vehicle, the user must visually verify that the system accurately read the license plate and, if so, must then contact Dispatch to verify accuracy of the hit – that the vehicle is actually listed as stolen. Only then does the user take action.

Unless a hit has been flagged for investigation and exported from the database for this purpose, all captured data is automatically deleted after 90 days, per department retention policy.

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?

Formatted: Font:

Formatted: Heading 3, Space Before: 0 pt, After: 0 pt, Line spacing: single

Formatted: Font: Not Bold

~~ALPR systems are used in Patrol on a daily basis by authorized sworn users (see 2.5 above). Supervisors within each precinct determine when ALPR-equipped vehicles will be on patrol and by which trained personnel.~~

In-car video systems with enabled ALPR will be used in Patrol on a daily basis by authorized sworn users (see 2.5 above).

4.4 How often will the technology be in operation?

Formatted: Font:

Formatted: Font: Not Bold

Formatted: Heading 3, Space Before: 0 pt, After: 0 pt, Line spacing: single

~~ALPR equipped vehicles are deployed within precincts based on operational need, as determined by supervisors within each precinct. See 4.3 and SPD Policy 16.170 (see 3.3 above).~~

In-car video systems with enabled ALPR will be used in Patrol on a daily basis by authorized sworn users (see 2.5 above).

Formatted: Indent: Left: 0"

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

Formatted: Font:

Formatted: Font: Not Bold

Formatted: Heading 3, Space Before: 0 pt, After: 0 pt, Line spacing: single

~~SPD has eight ALPR systems that are permanently installed on eight vehicles. The systems are temporarily collecting data when in use.~~

Fleet-wide ALPR is a component of permanently installed in-car video.

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?

Formatted: Font:

Formatted: Heading 3, Space Before: 0 pt, After: 0 pt, Line spacing: single

Formatted: Font: Not Bold

~~Seven of the eight ALPR-equipped patrol cars are marked as police vehicles. One patrol car is unmarked; however, the cameras are visible to the naked eye. In essence, the ALPR cameras are visible to the public, in plain view.~~

~~Additional markings would not render the technology ineffective, as the technology is not used covertly.~~

Fleet-wide ALPR is a component of permanently installed in-car video. Most SPD vehicles which have in-car video units installed are clearly marked as police vehicles. In-car video with enabled ALPR is installed in ~~less than XX~~ a few unmarked SPD vehicles which also have in-car video units.

Commented [VCM1]: @Britt, James Can you please make adjustments here as needed?

Commented [BJ2R1]: I would need to work with Marcus Mendoza in Fleets to figure this out. But for vehicles with ICV, they are clearly police vehicles, even when "unmarked." Is this important to include?

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

Formatted: Font:

Formatted: Font: Not Bold

Formatted: Heading 3, Space Before: 0 pt, After: 0 pt, Add space between paragraphs of the same style

Formatted: Indent: Left: 0"

Only authorized users can access the data collected by ALPR. Per SPD Policy 16.170, authorized users must access the data only for active investigations and all activity by users in the system is logged and auditable. SPD personnel within specific investigative units have access to ALPR data during its retention window of 90 days, during which time they can reference the data if it relates to a specific investigation.

Data removed from the system/technology and entered into investigative files is securely input and used on SPD's password-protected network with access limited to 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.

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

ALPR systems are operated and used only by SPD personnel.

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

Users can only access the equipment for purposes earlier outlined (see 1.0) – recovery of lost or stolen property, to assist with active investigations, Scofflaw Law enforcement, and parking enforcement. Per SPD Policy 16.170, "ALPR may be used during routine patrol or any criminal investigation," and users can access " Patrol ALPR data only when the data relates to a specific criminal investigation."

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.)?

~~Individuals can only access the ALPR system via unique login credentials. Hardware systems can only be accessed in-vehicle (which are assigned by superiors for each shift), and software systems can only be accessed in-vehicle or on-site of SPD. As previously noted, all activity in the system is logged and can be audited.~~

~~Further, City IT manages SQL backends that purge ALPR data at the required intervals (90 days). A record of the purge is generated and accessible at any time for verification of purges.~~

Formatted: Indent: Left: 0"

Formatted: Indent: Left: 0"

Individuals can only access the ALPR system via unique login credentials. Hardware systems can only be accessed in-vehicle. As previously noted, all activity in the system is logged and can be audited.

SPD's Audit Unit can conduct an audit of the any system at any time. The Office of Inspector General and the federal monitor can also access all data and audit for compliance at any time.

5.0 Data Storage, Retention and Deletion

5.1 How will data be securely stored?

~~All data collected from the ALPR system is stored, maintained, and managed on premises. Retention is automated, such that unless a record is identified as being related to a criminal investigation and exported in support of that investigation, all ALPR data is deleted after 90 days. No backup data is captured or retained.~~

All data collected from the ALPR system is stored, maintained, and managed in a CJIS certified evidence retention platform. Retention is automated, such that unless a record is identified as being related to a criminal investigation and exported in support of that investigation, all ALPR data is deleted after 90 days. No backup data is captured or retained.

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

~~ALPR systems maintain access logs on backend servers that are accessible for audit to any appropriate authority, including the Office of Inspector General and the Federal Monitor.~~

SPD's Audit Unit can conduct an audit of any SPD system at any time. In addition, the Office of Inspector General can access all data and audit for compliance at any time.

SPD conducts periodic reviews of audit logs and they are available for review at any time by the Seattle Intelligence Ordinance Auditor under the City of Seattle Intelligence Ordinance. The software automatically alerts users of data that must be deleted under legal deletion requirements such as 28 CFR Part 23.

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

Formatted: Indent: Left: 0"

Once a license plate has been read, this data is automatically retained. Any action taken at the scene as a result of a HotList hit can be contested by individuals. Users may make notes in records about license plate data captured that reflects that the hit is a misread, or that the hit was in error. The data unrelated to a specific investigation is retained for 90 days.

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

Seattle City IT, in conjunction with SPD's ALPR administrator is responsible for ensuring compliance with data retention requirements. Additionally, external audits by OIG and the Federal Monitor can review and ensure 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?

Formatted: Indent: Left: 0"

SPD has no data sharing partners for ALPR. No person, outside of SPD, has direct access to the PIPS system or the data while it resides in the system or technology.

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

Data may be shared without 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 by the ALPR 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 provide by SPD Policy 12.055. This sharing may include discrete pieces of data related to specific investigative files collected by the ALPR system.

6.2 Why is data sharing necessary?

~~Data sharing is necessary for SPD to fulfill its mission as a law enforcement agency and to comply with legal requirements.~~

Formatted: Indent: Left: 0"

Data sharing is frequently necessary during the course of a criminal investigation to follow up on leads and gather information on suspects from outside law enforcement agencies. Cooperation between law enforcement agencies is an essential part of the investigative process.

Products developed using this information may be shared with other law enforcement agencies. All products created with the information used in this project will be classified as Law Enforcement Sensitive. Any bulletins will be marked with the following restrictions: LAW ENFORCEMENT SENSITIVE — DO NOT LEAVE PRINTED COPIES UNATTENDED — DISPOSE OF IN SHREDDER ONLY – NOT FOR PUBLIC DISPLAY OR DISTRIBUTION — DO NOT FORWARD OR COPY.

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

Yes ☒ No ☐

Formatted: Indent: Left: 0"

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 28 CFR Part 20. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260, and RCW Chapter 10.97.

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?

Research agreements must meet the standards reflected in SPD Policy 12.055. Law enforcement agencies receiving criminal history information are subject to the requirements of 28 CFR 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 [system or technology] 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.

Formatted: Heading 3, Space After: 0 pt, Line spacing: single

System users are trained to visually verify accuracy, comparing a license plate hit to the physical plate/vehicle that the system read before taking any action. If they note a misread, they can enter a note into the system recognizing the read, as such. If they cannot verify visually, no action is taken.

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

Formatted: Heading 3, Space After: 0 pt, Line spacing: single

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?

Formatted: Heading 3, Space After: 0 pt, Line spacing: single

ALPR use is not legally constrained at the local, state, or federal level. Instead, retention of data is restricted. SPD retains license plate data that is not case specific (i.e., related to an investigation) for 90 days.

Case specific data is maintained for the retention period applicable to the specific case type.

Formatted: Indent: Left: 0"

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

Formatted: Font:

Formatted: Heading 3, Line spacing: single

Formatted: Font: Not Bold

~~For example, police department responses may include references to the Seattle Police Manual.~~

~~Users are trained in how to use the system and how to properly access data by other trained SPD users. No formal training exists beyond this. The TESU administrator confirms the training before providing access to new users.~~

~~SPD Policy 12.050 mandates that all employees, including ALPR users, complete Security Awareness Training (Level 2), and all employees also complete City Privacy Training.~~

SPD Policy 12.050 mandates that all employees receive Security Awareness Training (Level 2), and all employees also receive City Privacy Training. All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), many of which contain specific privacy requirements. 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.

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.

Formatted: Font:

Formatted: Heading 3, Line spacing: single

Formatted: Font: Not Bold

Each component of data collected, on its own, does not pose a privacy risk. Paired with other known or auditable information, however, an individual may be able to personally identify owners of vehicles, and then use that information to determine, to a certain degree, where specific vehicles have been located. Because SPD's fleet-wide ALPR cameras are not fixed in location and records are only retained for 90 days, privacy risk is substantially mitigated because of the limited ability to identify vehicle patterns.

Per SPD Policy 16.170, general users of ALPR are restricted from accessing the data, except as it relates to a specific criminal investigation. Any activity by a user to access this information is logged and auditable. The PRA requires release of collected ALPR data, however, making it possible for members of the general public to make those identification connections on their own if they have access to the information necessary to do so, such as an independent knowledge of a particular individual's license plate number.

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?

Formatted: Heading 3, Line spacing: single

Formatted: Indent: Left: 0"

As mentioned in 7.3, the data could be used to personally identify individuals; however, SPD policy prohibits the use of data collected by ALPR to be used in any capacity beyond its relation to a specific criminal investigation or parking enforcement action. Additionally, all collected data that is not relevant to an active investigation is deleted after 90 days of collection.

8.0 Monitoring and Enforcement

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

Data collected by ALPR is only disclosed pursuant to the public under the PRA. The only data available for disclosure is that data which remains in the system within the 90-day retention window.

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 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.

Formatted: Font:

Formatted: Heading 3, Space After: 0 pt, Line spacing: single

Formatted: Font: Not Bold

~~The ALPR system does not self-audit. Instead, third party audits exist, as follows: 1) The ALPR administrator has the responsibility of managing the user list and ensuring proper access to the system; 2) The Federal Monitor can conduct an audit at any time; and 3) the OIG can also conduct an audit. Violations of policy may result in referral to Office of Professional Accountability (OPA).~~

The ALPR system does not self-audit. Instead, third party audits exist, as follows: 1) The ALPR administrator has the responsibility of managing the user list and ensuring proper access to the system; 2) The Federal Monitor can conduct an audit at any time; and 3) the OIG can also conduct an audit. Violations of policy may result in referral to Office of Professional Accountability (OPA).

SPD's Audit Unit personnel can also conduct audits of all data collection software and systems. Additionally, any appropriate auditor, including the Office of Inspector General and the federal monitor can audit for compliance at any time.

Formatted: Font: 11 pt, Not Bold, Font color: Auto, Not All caps

Formatted: No Spacing, Space After: 0 pt, Line spacing: single

Formatted: Font: 18 pt, Bold

Formatted: Indent: Left: 0"

Financial Information

Purpose

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

Formatted: Font:

Formatted: No Spacing

Formatted: Font:

1.0 Fiscal Impact

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

Formatted: Font: (Default) +Body (Calibri)

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
~~2006 (3M – purchased by Neology in 2016)~~	~~2006~~	~~Unable to locate – however, costs in 2015 = $167,694.17~~			~~SPD Budget~~

Formatted: No Spacing

Notes:

~~This reflects the date for which SPD has some acquisition costs for 3M. The PIPS ALPR system dates back to 2006, for which limited acquisition cost data is available.~~

Formatted: Font: Not Bold

Formatted: No Spacing

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

Notes:

Respond to question 7.3 here

Formatted: Indent: Left: 0"

1.3 Cost savings potential through use of the technology

Respond to question 1.3 here

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

Seattle Police Foundation Grant

Formatted: Indent: Left: 0"

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.

Formatted: Font:

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.

Formatted: No Spacing

Agency, municipality, etc.	Primary contact	Description of current use
Washington State Patrol		

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
Bryce Newell, PhD	Brycenewell@uky.edu	“Transparent Lives and the Surveillance State: Policing, New Visibility, and Information Policy” – A Dissertation

3.0 White Papers or Other Documents

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

Formatted: Indent: Left: 0"

Automated License Plate Recognition Systems: Policy and Operational Guidance for Law Enforcement	US Department of Justice (federally-funded grant report)	https://www.ncjrs.gov/pdffiles1/nij/grants/239604.pdf

Formatted: Indent: Left: 0"

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.

Formatted: No Spacing

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.

Formatted: Indent: Left: 0"

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

~~Without appropriate policy, license plate data could be paired with other identifiable information about individuals that could be used to identify individuals without reasonable suspicion of having committed a crime, or to data mine for information that is not incidental to any active investigation. SPD Policy 16.170 mitigates this concern by limiting operation to solely routine patrol or criminal investigation.~~

~~1.3 What does your department define as the most important racially equitable community outcomes related to the implementation of this technology~~?

~~Trust in SPD is impacted by its treatment of all individuals. Equity in treatment, regardless of actual or perceived race, gender, sex, sexual orientation, country of origin, religion, ethnicity, age, and ability is critical to establishing and maintaining trust.~~

~~Per the 2016 Race and Social Justice Initiative Community Survey, measuring "the perspectives of those who live, work, and go to school in Seattle, including satisfaction with City services, neighborhood quality, housing affordability, feelings about the state of racial equity in the city, and the role of government in addressing racial inequities," 56.1% of African American/Black respondents, 47.3% of Multiracial respondents, and 47% of Indian/Alaska Native respondents have little to no confidence in the police to do a good job enforcing the law, as compared with 31.5% of White respondents. Further, while 54.9% of people of color have a great deal or fair amount of confidence in the police to treat people of color and White people equally, 45.1% of people of color have little to no confidence in the police to treat people equitably. This is contrasted with White respondents, of which 67.5% have a great deal or fair amount of confidence in the police to treat people of color and White people equally. This may be rooted in feelings of disparate types of contact with the police, across racial groups. While 14.3% of White respondents, 14.7% of Asian/Pacific Islander respondents, and 16.7% of Latino/Hispanic respondents reported being questioned by the police, charged, or arrested when they had not committed a crime, some communities of color reported much higher rates (American Indian/Alaska Native -52.7%; Black/African American - 46.8%; and Multiracial - 36.8%) of this type of contact with the criminal justice system.~~

~~As it relates to ALPR, it is important that SPD continue to follow its policy of limiting use of the technology to strictly routine patrol or criminal investigation, as well as limiting access to ALPR data to only instances in which it relates to a specific criminal investigation. Further, continuing to audit the system on a regular basis, provides a measure of accountability. In doing so, SPD can mitigate the appearance of disparate treatment of individuals based on factors other than true criminal activity.~~

~~1.4 What racial equity opportunity area(s) will be affected by the application of the technology?~~

~~☐ Education~~ ~~☐ Community Development~~ ~~☐ Health~~ ~~☐ Environment~~ Without appropriate policy, license plate data could be paired with other identifiable information about individuals that could be used to identify individuals without reasonable suspicion of having committed a crime, or to data mine for information that is not incidental to any active investigation. SPD Policy 16.170 mitigates this concern by limiting operation to solely routine patrol or criminal investigation.	~~☒ Criminal Justice~~ ~~☐ Jobs~~ ~~☐ Housing~~ ~~☐ Other~~

Formatted: Indent: Left: 0"

Deleted Cells

Formatted: Default Paragraph Font

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.

Formatted: Indent: Left: 0"

Trust in SPD is impacted by its treatment of all individuals. Equity in treatment, regardless of actual or perceived race, gender, sex, sexual orientation, country of origin, religion, ethnicity, age, and ability is critical to establishing and maintaining trust.

Per the 2016 Race and Social Justice Initiative Community Survey, measuring "the perspectives of those who live, work, and go to school in Seattle, including satisfaction with City services, neighborhood quality, housing affordability, feelings about the state of racial equity in the city, and the role of government in addressing racial inequities," 56.1% of African American/Black respondents, 47.3% of Multiracial respondents, and 47% of Indian/Alaska Native respondents have little to no confidence in the police to do a good job enforcing the law, as compared with 31.5% of White respondents. Further, while 54.9% of people of color have a great deal or fair amount of confidence in the police to treat people of color and White people equally, 45.1% of people of color have little to no confidence in the police to treat people equitably. This is contrasted with White respondents, of which 67.5% have a great deal or fair amount of confidence in the police to treat people of color and White people equally. This may be rooted in feelings of disparate types of contact with the police, across racial groups. While 14.3% of White respondents, 14.7% of Asian/Pacific Islander respondents, and 16.7% of Latino/Hispanic respondents reported being questioned by the police, charged, or arrested when they had not committed a crime, some communities of color reported much higher rates (American Indian/Alaska Native -52.7%; Black/African American - 46.8%; and Multiracial - 36.8%) of this type of contact with the criminal justice system.

As it relates to ALPR, it is important that SPD continue to follow its policy of limiting use of the technology to strictly routine patrol or criminal investigation, as well as limiting access to ALPR data to only instances in which it relates to a specific criminal investigation. Further, continuing to audit the system on a regular basis, provides a measure of accountability. In doing so, SPD can mitigate the appearance of disparate treatment of individuals based on factors other than true criminal activity.

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

☒ all Seattle neighborhoods

Formatted: No Spacing

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont

Formatted: Indent: Left: 0"

☐ International District
☐ Interbay
☐ North
☐ Northeast

☐ 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.

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

Formatted: No Spacing

Formatted: Indent: Left: 0"

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

City of Seattle demographics: White - 69.5%; Black or African American - 7.9%; Amer. Indian & Alaska Native - 0.8%; Asian - 13.8%; Native Hawaiian & Pacific Islander - 0.4; Other race - 2.4%; Two or more races - 5.1%; Hispanic or Latino ethnicity (of any race): 6.6%; Persons of color: 33.7%.

King County demographics: White – 70.1%; Black or African American – 6.7%; American Indian & Alaskan Native – 1.1%; Asian, Native Hawaiian, Pacific Islander – 17.2%; Hispanic or Latino (of any race) – 9.4%

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?

Per SPD Policy 16.170, "Before employees operate the ALPR system or access ALPR data, they will complete Department training on the proper and lawful use of the system." 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.

Also, by equipping all in-car video throughout the department with ALPR, deployment of this system becomes non-discretionary. When ALPR is deployed based on where calls for police service are, implicit biases are removed from consideration in this regard.

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?

Historically targeted communities have often been denied the same opportunities for information privacy as the majority populations. Data sharing has the potential to be a contributing factor to structural racism and thus creating a disparate impact on historically targeted communities. In an effort to mitigate this possibility, SPD has established policies regarding the dissemination of data in connection with criminal prosecutions, Washington Public Records Act (Chapter 42.56 RCW), and other authorized researchers. Further, 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.

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?

Formatted: Indent: Left: 0"

As with decisions around data sharing, data storage and retention have similar potential for disparate impact on historically targeted communities.

Further, 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.

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.

Without appropriate policy, license plate data could be paired with other identifiable information about individuals that could be used to identify individuals without reasonable suspicion of having committed a crime, or to data mine for information that is not incidental to any active investigation. SPD Policy 16.170 mitigates this concern by limiting operation to solely routine patrol or criminal investigation. 90-day data retention also mitigates the risk of improper identification of community members.

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.

1. Date	2.	3.

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	
Time	
Capacity	
Link to URL Invite	

2.2 Scheduled focus Group Meeting(s)

Meeting 1

Community Engaged	
Date	

Formatted: Indent: Left: 0"

Meeting 2

Community Engaged	
Date	

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].

Formatted: Indent: Left: 0"

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

Formatted: Strong

Formatted: Strong

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?

Respond here.

Formatted: Indent: Left: 0"

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.

Formatted: Indent: Left: 0"

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 ~~outreach plan (Step 2c).~~

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

Formatted: No Spacing

Formatted: Emphasis

Formatted: Emphasis, Font: 18 pt, Bold

Formatted: Indent: Left: 0"

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.

Formatted: Indent: Left: 0"

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

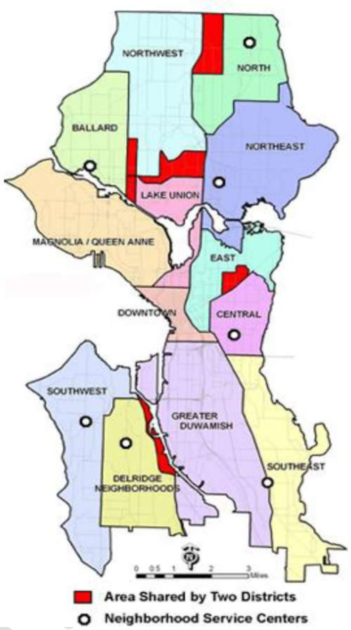
RET: "racial equity toolkit"

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.

Formatted: Indent: Left: 0"

Appendix B: Public Comment Analysis

Appendix C: Public Comment Demographics

Appendix D: Comment Analysis Methodology

Appendix E: Questions and Department Responses

Appendix F: Public Outreach Overview

Appendix G: Meeting Notice(s)

Appendix H: Meeting Sign-in Sheet(s)

Appendix I: All Comments Received from Members of the Public

Appendix J: Letters from Organizations or Commissions

Appendix K: Supporting Policy Documentation

Appendix L: CTO Notification of Surveillance Technology