POWERFUL TECHNOLOGY SOLUTIONS
FOR THE CITY AND PUBLIC WE SERVE

2018 Surveillance Impact Report

AUTOMATED LICENSE PLATE RECOGNITION (ALPR) (PATROL)

SEATTLE POLICE DEPARTMENT

October 8, 2018

Seattle
Information Technology

CONTENTS

SURVEILLANCE IMPACT REPORT OVERVIEW 4

HOW THIS DOCUMENT IS COMPLETED 4

PRIVACY IMPACT ASSESSMENT 5

PURPOSE 5

WHEN IS A PRIVACY IMPACT ASSESSMENT REQUIRED? 5

1.0 ABSTRACT 6

1.1 PLEASE PROVIDE A BRIEF DESCRIPTION (ONE PARAGRAPH) OF THE PURPOSE AND PROPOSED USE OF THE PROJECT/TECHNOLOGY. 6

1.2 EXPLAIN THE REASON THE PROJECT/TECHNOLOGY IS BEING CREATED OR UPDATED AND WHY THE PIA IS REQUIRED. 7

2.0 PROJECT / TECHNOLOGY OVERVIEW 7

2.1 DESCRIBE THE BENEFITS OF THE PROJECT/TECHNOLOGY. 8

2.1 CONTINUED 9

2.2 PROVIDE ANY DATA OR RESEARCH DEMONSTRATING ANTICIPATED BENEFITS. 10

2.3 DESCRIBE THE TECHNOLOGY INVOLVED. 11

2.4 DESCRIBE HOW THE PROJECT OR USE OF TECHNOLOGY RELATES TO THE DEPARTMENT'S MISSION. 12

2.5 WHO WILL BE INVOLVED WITH THE DEPLOYMENT AND USE OF THE PROJECT / TECHNOLOGY? 12

3.0 USE GOVERNANCE 13

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. 13

3.2 LIST THE LEGAL STANDARDS OR CONDITIONS, IF ANY, THAT MUST BE MET BEFORE THE PROJECT / TECHNOLOGY IS USED. 13

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. 14

4.0 DATA COLLECTION AND USE 15

DRAFT

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. 15
5.0 DATA STORAGE, RETENTION AND DELETION 19
6.0 DATA SHARING AND ACCURACY 20
7.0 LEGAL OBLIGATIONS, RISKS AND COMPLIANCE 22
8.0 MONITORING AND ENFORCEMENT 24
FINANCIAL INFORMATION 25
PURPOSE 25
1.0 FISCAL IMPACT 25
EXPERTISE AND REFERENCES 27
PURPOSE 27
1.0 OTHER GOVERNMENT REFERENCES 27
2.0 ACADEMICS, CONSULTANTS, AND OTHER EXPERTS 27
3.0 WHITE PAPERS OR OTHER DOCUMENTS 28
RACIAL EQUITY TOOLKIT AND ENGAGEMENT FOR PUBLIC COMMENT WORKSHEET 29
PURPOSE 29
ADAPTION OF THE RET FOR SURVEILLANCE IMPACT REPORTS 29
RACIAL EQUITY TOOLKIT OVERVIEW 29
RACIAL EQUITY TOOLKIT: TO ASSESS POLICIES, INITIATIVES, PROGRAMS, AND BUDGET ISSUES 29
1.0 SET OUTCOMES 30
2.0 INVOLVE STAKEHOLDERS, ANALYZE DATA 32
3.0 DETERMINE BENEFIT AND/OR BURDEN 34
4.0 ADVANCE OPPORTUNITY OR MINIMIZE HARM 35

DRAFT

5.0 EVALUATE, RAISE RACIAL AWARENESS, BE ACCOUNTABLE 36
6.0 REPORT BACK 37
PRIVACY AND CIVIL LIBERTIES ASSESSMENT 38
PURPOSE 38
WORKING GROUP PRIVACY AND CIVIL LIBERTIES ASSESSMENT 38
APPENDIX A: GLOSSARY 39
APPENDIX B: PUBLIC COMMENT DEMOGRAPHICS AND OVERVIEW 41
APPENDIX C: PUBLIC MEETING NOTICE(S) 41
APPENDIX D: MEETING SIGN-IN SHEET(S) 41
APPENDIX E: MEETING TRANSCRIPT(S) 41
APPENDIX F: LETTERS FROM ORGANIZATIONS 41
APPENDIX H: EMAILS FROM THE PUBLIC 41
APPENDIX I: LETTERS FROM THE PUBLIC 41

DRAFT

SURVEILLANCE IMPACT REPORT OVERVIEW

The Seattle City Council passed Ordinance 125376, also referred to as the "Surveillance Ordinance", on September 1, 2017. This Ordinance has implications for the acquisition of new technologies by the City, and technologies that are already in use that may fall under the new, broader definition of surveillance.

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

As Seattle IT and department staff complete the document, they should keep the following in mind.

- 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.
- 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.

DRAFT

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.

DRAFT

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 uses Automated License Plate Reader (ALPR) technology to recover stolen vehicles, to locate subjects of Amber and Silver Alerts and fugitives where vehicle license plate information is available, to assist with active investigations, to facilitate the flow of traffic (by monitoring and enforcing City parking restrictions) and for Scofflaw Ordinance enforcement. This Surveillance Impact Report focuses on SPD use of Patrol 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 stored ALPR data within the 90-day retention period to assist in criminal investigations by identifying and locating involved vehicles, including locating subjects of Amber and Silver Alerts.

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

SPD has nineteen vehicles with ALPR. Eleven of these are Patrol vehicles and eight are Parking Enforcement vehicles. The eleven Patrol vehicles are distributed across SPD's five precincts, the Canine and Major Crimes Units also each have an ALPR-equipped vehicle. Although ALPR use by Patrol differs from ALPR use for Parking Enforcement in some respects as described in this Surveillance Impact Report and in the Parking Enforcement Systems (including ALPR) Surveillance Impact Report, all rules and policies that govern ALPR use by SPD as mentioned in the Parking Enforcement Systems Surveillance Impact Report are applicable in the same manner as they are when ALPR is utilized by Patrol.

SPD does not pool ALPR data with other federal agencies. However, ALPR data is subject to the Public Records Act.

The surveillance technology in this Surveillance Impact Report (SIR) is:

1. **Neology PIPS** mobile license plate recognitions system, which is installed in eleven Patrol vehicles.
2. **Neology Back Office System Software (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.

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' vehicles and determine where they were parked at a given time, track the movements of innocent individuals, or be pooled with ALPR data from other agencies.

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

DRAFT

2.1 Describe the benefits of the project/technology.

The benefit of ALPR is many-fold. Patrol ALPR and Parking Enforcement ALPR assist the City in locating and recovering stolen vehicles. Parking Enforcement ALPR assists the City in managing the flow of traffic (by monitoring and enforcing City Traffic Code provisions). Additionally, both ALPR systems may assist 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.

SPD uses ALPR to recover stolen vehicles, which are often used by thieves in committing other crimes. SPD uses ALPR to locate subjects of Amber and Silver Alerts, fugitives where vehicle license plate information is available, and ALPR has proven to be an essential tool for locating subjects of Amber and Silver Alerts and fugitives where vehicle license plate information is available and in investigating crime. Examples include:

- A murder, in which the victim who, while dropping off passengers, was confronted and shot. A search of ALPR data located images of the vehicle plate the day of and day after the homicide. The images showed that the vehicle had been painted from black to gold in an attempt to conceal it. This assisted in apprehending the suspect.

- SPD used ALPR to identify a suspect's vehicle parked in the vicinity of a murder. Security video from surrounding businesses showed the suspect vehicle being driven in the area, which was critical in the arrest and charging of the two responsible suspects.

- SPD obtained a partial plate and a description of the car in a drive-by-shooting with three innocent victims . SPD ran several partial plate searches and found one in the ALPR system that had been in the area of the shooting at the time. The vehicle matched the description and led to identification of the vehicle and ultimately to the arrest of the shooting suspects.

- A victim at a charity-operated homeless shelter was threatened and nearly stabbed by an individual who was known only by his first name. The victim reported that the suspect had stabbed people before, was extremely violent, and had left the scene in an agitated state. The victim was able to provide a partial license plate, which with other description information, enabled SPD to use the ALPR database to determine the car was routinely parked under a nearby overpass in the middle of the night. SPD then located the vehicle and the suspect before he hurt anyone else.

- A violent robbery in Tukwila involved a stolen VW Toureg. The suspects in that crime were involved in subsequent incidents including gun theft and a road rage incident in which a victim was shot at. Using ALPR data, SPD found several locations where the vehicle had been in the North Precinct area. Photos from the ALPR database provided pictures of the current color of the vehicle as the registration reported a different color. A bulletin describing the vehicle and indicating the possible location assisted SPD in locating the vehicle in north Seattle and arresting the suspects in these violent crimes.

2.1 Continued

- Snohomish County Detectives asked for assistance locating a stranger rape suspect. Images of the suspect's vehicle had been captured on a convenience store security camera when the victim had been picked up. The security video allowed SPD to read the license plate of the potential suspect vehicle. Using the ALPR system, SPD found that the vehicle had parked several times in a business parking lot in Seattle around the same time every day. This was most likely a work location for a potential suspect. The ALPR led to identification and arrest of the suspect, who worked at the Seattle business.

- SPD received reports that a male exposed himself to teen-aged-girls near a local high school. Using ALPR, SPD was able to determine that a vehicle matching the description and reported license plate information had been parked near the high school at the time of the incidents.

DRAFT

2.2 Provide any data or research demonstrating anticipated benefits.

Research studies:

- Gierlack, Keith, et al. *License Plate Readers for Law Enforcement: Opportunities and Obstacles*. RAND Corporation. https://www.ncjrs.gov/pdffiles1/nij/grants/247283.pdf
- Roberts, David & Meghann Casanova. *Automated License Plate Recognition Systems: Policy and Operational Guidance for Law.* U.S. Department of Justice. https://www.ncjrs.gov/pdffiles1/nij/grants/239604.pdf

General news reporting about ALPR Benefits:

- "Auto thefts up 10 percent in Seattle's North Police Precinct". Sep. 13, 218. KIRO News. https://www.kiro7.com/news/local/auto-thefts-up-10-percent-in-seattles-north-police-precinct/832872563
- "Suspect in New York murder arrested in Spokane". Kelsie Morgan. Jun. 21, 2018. KXLY News. https://www.kxly.com/news/local-news/suspect-in-new-york-murder-arrested-in-spokane/756515490
- "Man suspect of sexual assault of child arrested for brazen Fremont home-invasion robbery". Mark Gomez. Sep 13, 2018. Mercury News. https://www.mercurynews.com/2018/09/13/fremont-police-arrest-man-suspected-of-home-invasion-robbery-sexual-assault-of-child/
- "Man Sentenced to 7 Years for Northeast DC Gunpoint Carjacking of Nun". Sophia Barnes. Sep 7, 2018. NBC Washington. https://www.nbcwashington.com/news/local/Man-Sentenced-to-7-Years-for-Carjacking-Nun-in-Northeast-DC-Brookland-492714631.html
- "License plate readers help Miami Beach police crack down on crime". Andrew Perez. Jul 31, 2018. ABC 10. https://www.local10.com/news/florida/miami-beach/license-plate-readers-help-miami-beach-police-crack-down-on-crime
- "License plate readers helping police in many ways". Tony Terzi. Sep 5, 2018. FOX 61. https://fox61.com/2018/09/05/license-plate-readers-helping-police-in-many-ways/
- "License plate reader technology scores break in hit-and-run probe". Paul Mueller. Sep 20, 2018. CBS 12. https://cbs12.com/news/local/license-plate-reader-technology-scores-break-in-hit-and-run-probe
- "License-plate scanners result in few 'hits,' but are invaluable in solving crimes, police say". Karen Farkas. Dec 4, 2017. Cleveland.com. https://www.cleveland.com/cuyahoga-county/index.ssf/2017/12/license_plate_readers_result_in_few_hits_but_are_invaluable_in_solving_crimes_police_say.html

2.3 Describe the technology involved.

ALPR hardware consists of high definition infrared digital cameras that are mounted on eleven 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 ALPR-equipped Patrol vehicles 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 so that the cameras capture the images and filter the reads through the 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 Patrol 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. Similar ALPR data collected by three ALPR-equipped Parking Enforcement boot vans equipped with Paylock Bootview software is also stored with Patrol ALPR data in BOSS. After 90 days, all data collected by the patrol and boot van ALPR systems is automatically deleted unless specific data has been exported as serving an investigative purpose – in which case, it is included in an investigation file (see the Surveillance Impact Report for Parking Enforcement Systems (including ALPR) for further information).

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. ALPR systems can be used during routine patrol or specific to a criminal investigation e.g., to locate a stolen vehicles.

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. ALPR- equipped vehicles in the Canine and Major Crimes Unit respond to calls and matters City-wide, thus providing coverage across the City.

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. Officers assigned to the two specialty units, who have been trained in the use of ALPR, may operate it.

The Technical and Electronic Support Unit (TESU), a unit within SPD maintains administrative control of much of SPD's physical technology. The unit staff is knowledgeable about investigative and forensic technology. TESU's mission is to provide technical assistance to Detectives and Officers in connection with investigations. The BOSS ALPR administrator is a member of TESU. The ALPR administrator monitors and manages user access to the PIPS ALPR system for Patrol. The ALPR administrator purges users from system access when they leave the Department. 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.

3.0 USE GOVERNANCE

Provide an outline of any rules that will govern the use of the project / technology. Please note: non-City entities 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. 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 specifies that the ALPR system administrator will be a member of the Technical and Electronic Support Unit (TESU). It further 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. Records of these requests are purged after 90 days.

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.

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 ALPR-equipped Patrol vehicles.

DRAFT

4.0 DATA COLLECTION AND USE

Provide information about the policies and practices around the collection and use of the data collected.

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 from the Washington State Patrol that contains national stolen vehicle plate data published daily by the FBI. The Washington State Patrol places the HotList file on a server available through ACCESS to those agencies that have a specific and signed agreement with WSP to access and use the information. The receiving local law enforcement may supplement the list with additional information, such as vehicles sought with reasonable suspicion that they are involved in an incident or vehicles sought pursuant to a warrant. (see the Surveillance Impact Report for Parking Enforcement Systems (including ALPR) for further information regarding ALPR use by Parking Enforcement Officers).

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

When the ALPR system registers a hit, a match to a 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. Data related to a flagged hit is downloaded and maintained with the investigation file for the retention period related to the incident type.

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?

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. Detectives may access ALPR data in connection with investigations of criminal incidents based on reasonable suspicion.

4.4 How often will the technology be in operation?

ALPR equipped vehicles are deployed within precincts and Canine and Major Crimes Units based on operational need, as determined by supervisors within each precinct or specialty unit. (See SPD Policy 16.170, 3.3 and 4.3 above).

16.170 - Automatic License Plate Readers
Effective Date: 8/15/2012
16.170-POL
This policy applies to the use of automatic license plate readers (ALPR) by Department employees.
1. Criminal Intelligence Section has Operational Control
The ALPR system administrator will be a member of the Technical and Electronic Support Unit (TESU).
2. Operators Must be Trained
Operators must be ACCESS certified and trained in the proper use of ALPR.
Training will be administered by TESU and Parking Enforcement, as applicable.
3. ALPR Operation Shall be for Official Department Purposes
ALPR may be used during routine patrol or any criminal investigation.
4. Only Employees With ACCESS Level 1 Certification May Access ALPR Data
Employees are permitted to access ALPR data only when the data relates to a specific criminal investigation.
A record of requests to review stored ALPR data will be maintained by TESU.

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

SPD has eleven patrol vehicles with ALPR cameras that are permanently installed. The vehicles are temporarily collecting data when in use. The data collected is maintained on the SPD internal BOSS ALPR system for 90 days or in investigative files for the retention period related to the incident type. (See 4.2 above).

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?

Ten of the eleven ALPR-equipped patrol cars are marked as police vehicles, and the cameras are visible to the naked eye. One patrol car is unmarked, and the camera is not visible to the naked eye.

Additional markings on the ten marked vehicles are unnecessary because the vehicles are plainly marked as police vehicles. Additional markings on the unmarked patrol vehicle would render it ineffective as an investigative tool.

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

Please do not include staff names; roles or functions only.

All data collected for Parking Enforcement systems are hosted on City SPD servers and are not accessible by vendors without knowledge and/or permission of City personnel. Unlike some ALPR systems, SPD's systems do not "pool" SPD's ALPR data with that collected by other agencies.

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. Please link memorandums of agreement, contracts, etc. that are applicable.

Access to the Patrol ALPR system front-end and back-end is limited to ALPR-trained officers, authorized SPD administrators, and authorized Seattle City IT administrators.

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– recovery of stolen vehicles 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 ALPR data may be accessed "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 backend that purges ALPR data at the required intervals (90 days). A record of the purge is generated and accessible at any time for verification of purges.

DRAFT

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. Unless a record is identified as being related to a criminal investigation and exported in support of that investigation prior to 90 days, 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 The Office of Inspector General may access all data and audit for compliance at any time.

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

Once a license plate has been read, this data is automatically retained. Any action taken as a result of a HotList hit can be contested by involved 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.

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 guaranteed by the Constitution of the United States and the State of Washington, including freedom of speech, press, association, and assembly; liberty of conscience the exercise of religion; the right to petition government for redress of grievances; and the 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?

Seattle City IT, in conjunction with SPD's ALPR administrator in the Technical and Electronic Support Unit, is responsible for ensuring compliance with data retention requirements. Additionally, external audits by OIG 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?

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 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 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 Mayor's 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.

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 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?

Please describe the process for reviewing and updating data sharing agreements.

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 ALPR 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.

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.

Individuals would not know that their information is collected inaccurately or erroneously in the normal course of ALPR data reading. This would only come to an individual's attention if a user acts on a hit received. Any action taken as a result of a HotList or other hit can be contested by involved individuals. Individuals have the right to challenge citations, alleged code violations, or criminal charges and provide correct 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?

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.

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

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. The TESU administrator confirms the training before providing access to new users.

SPD Policy 12.050 mandates that all employees, including ALPR users, who use terminals that have access to information in WACIC/NCIC files must be certified by completing complete Security Awareness Training (Level 2) with recertification testing required every two years, and all employees also complete City Privacy Training. Failure to comply with ACCESS/NCIC/WACIC user requirements can result in termination of the right to continue using ACCESS services.

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.

Please work with the Privacy Team to identify the specific risks and mitigations applicable to this project / technology.

Each component of data collected, on its own, does not pose a privacy risk. Paired with other known or obtainable 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 ALPR cameras are few in number, not fixed in location, vehicles equipped with ALPR generally do not follow the same routes, and the records not related to a specific incident 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 stored data, except as it relates to a specific criminal investigation. Any activity by a user to access this information is logged and auditable. The Washington Public Records Act requires release of collected ALPR data, however, making it possible for members of the 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?

Examples might include a push of information out to individuals that is unexpected and appears to be intrusive, or an engagement with a third party to use information derived from the data collected, that is not explained in the initial notification.

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 90 days after collection.

DRAFT

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 that 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."

Discrete pieces of data collected by 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 SPD Policy 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 devices.

Any requests for disclosure are logged by SPD's Crime Records Unit or Legal Unit, as appropriate . 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 logged in SPD's GovQA system and 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 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 Office of Inspector General (OIG) can conduct an audit at any time. Violations of policy may result in referral to Office of Professional Accountability (OPA).

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
2006 ($3M – purchased by Neology in 2016)	2006	Unable to locate record of initial acquisition. However, costs 2015-2018 $217,297.47			SPD Budget

Notes:

The PIPS ALPR system dates back to 2006, for which limited initial acquisition cost data is available. More recent costs are identified.

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
N/A				

Notes:

N/A

DRAFT

1.3 Cost savings potential through use of the technology

These are not quantified; however, potential cost savings may result from enhanced patrol efficiency. The technology increases investigative efficiency by reducing the need to canvass neighboring residences and businesses in efforts to identify involved vehicles following an incident. It may reduce distractions for officers while driving because they do not have to visually scan license plates in search of stolen vehicles.

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

N/A

DRAFT

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
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

DRAFT

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.

Title	Publication	Link
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
License Plate Readers for Law Enforcement: Opportunities and Obstacles	Rand Corporation	https://www.ncjrs.gov/pdffiles1/nij/grants/247283.pdf
Local Law Enforcement Jumps on the Big Data Bandwagon: Automated License Plate Recognition Systems, Information Privacy, and Access to Government Information	66 Maine Law Review 398, 2014 Bryce Clayton Newell	https://cpb-us-w2.wpmucdn.com/wpsites.maine.edu/dist/d/46/files/2014/06/03-Newell.pdf

DRAFT

RACIAL EQUITY TOOLKIT AND ENGAGEMENT FOR PUBLIC COMMENT WORKSHEET

PURPOSE

Departments submitting a SIR are required to complete an adapted version of the Racial Equity Toolkit ("RET").

1. To provide a framework for the mindful completion of the Surveillance Impact Reports 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.
2. To highlight and mitigate any impacts on racial equity from the adoption and the use of the technology.
3. To highlight and mitigate any disparate impacts on individuals or vulnerable communities.
4. To fulfill the public engagement requirements of the Surveillance Impact Report.

ADAPTION 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

RACIAL EQUITY TOOLKIT: TO ASSESS POLICIES, INITIATIVES, PROGRAMS, AND BUDGET ISSUES

The vision of the Seattle Race and Social Justice Initiative is to eliminate racial inequity in the community. To do this requires ending individual racism, institutional racism and structural racism. The Racial Equity Toolkit 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.

WHEN DO I USE THIS TOOLKIT?

Early. Apply the toolkit early for alignment with departmental racial equity goals and desired outcomes.

HOW DO I USE THIS TOOLKIT?

With inclusion. The analysis should be completed by people with different racial perspectives.

Step by step. The Racial Equity Analysis is made up of six steps from beginning to completion:

Please refer to the following resources available on the Office of Civil Rights' website here: Creating effective community outcomes; Identifying stakeholders & listening to communities of color; Data resources

DRAFT

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?

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.

An additional potential civil liberties concern is that the SPD would over-surveil vulnerable or historically targeted communities, deploying ALPR to diverse neighborhoods more often than to other areas of the City.

DRAFT

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 affected 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
- ☒ Criminal Justice
- ☐ Jobs
- ☐ Housing
- ☐ Other

1.5 Are there impacts on:

- ☐ Contracting Equity
- ☐ Workforce Equity
- ☐ Immigrant and Refugee Access to Services
- ☐ Inclusive Outreach and Public Engagement
- ☒ Other

2.0 INVOLVE STAKEHOLDERS, ANALYZE DATA

2.1 Departmental conclusions about potential neighborhood impacts of the technology. Are the impacts on geographic areas? ☒ Yes ☐ No

Check all neighborhoods that apply *(see map of neighborhood boundaries in Appendix A: Glossary, under "Seattle Neighborhoods"):*

☒ All Seattle neighborhoods

- ☐ Ballard
- ☐ North
- ☐ Northeast
- ☐ Central
- ☐ Lake Union
- ☐ Southwest
- ☐ Southeast
- ☐ Delridge
- ☐ Greater Duwamish
- ☐ East District
- ☐ King County (outside Seattle)

☐ Outside King County. Please describe:

N/A

2.2 What are the racial demographics of those living in the area or impacted by the issue? *(see Stakeholder and Data Resources* here*.)*

The demographics for the City of Seattle: White - 69.5%; Black or African American - 7.9%; Amer. Indian & Alaska Native - 0.8%; Asian - 13.8%; Native Hawaiian & Other Pac. 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%.

STOP: Department should complete RET questions 2.3 – 6 and Appendices B-I AFTER completing their public comment and engagement requirements.

2.3 Have you completed the following steps to engage the public? If you have not completed these steps, pause here until public outreach and engagement has been completed. (*See OCR's RET worksheet here for more information about engaging the public at this point in the process to ensure their concerns and expertise are part of analysis.*)

☐ **Create a public outreach plan.** Residents, community leaders, and the public were informed of the public meeting and feedback options via:

- ☐ Email
- ☐ Mailings
- ☐ Fliers
- ☐ Phone calls
- ☐ Social media

☐ Other

☐ The following community leaders were identified and invited to the public meeting(s):

☐ American Civil Liberties Union (ACLU)
☐ CARE
☐ Northwest Immigrant Rights
☐ OneAmerica
☐ JACL
☐ For Seattle Police Department only, Community Police Commissions
☐ Other:

[Please describe]

☐ **Engagement for Public Comment #1**

Date of meeting: [Respond here.]

Location of meeting: [Respond here.]

Summary of discussion:

[Respond here, if applicable.]

☐ Full meeting transcript, including City attendees, community leaders in attendance, and attendee demographic data, is attached as an appendix to the SIR

☐ **Engagement for Public Comment #2**

Date of meeting: [Respond here.]

Location of meeting: [Respond here.]

Summary of discussion:

[Respond here, if applicable.]

☐ Full meeting transcript, including City attendees, community leaders in attendance, and attendee demographic data, is attached as an appendix to the SIR

☐ **Engagement for Public Comment #3 (if applicable)**

Date of meeting: [Respond here.]

Location of meeting: [Respond here.]

Summary of discussion:

[Respond here, if applicable.]

☐ Full meeting transcript, including City attendees, community leaders in attendance, and attendee demographic data, is attached as an appendix to the SIR

☐ **Collect public feedback via mail and email**

Number of feedback submissions received: [Respond here,]

Summary of feedback: [Respond here.]

Open comment period: [Respond here.]

☐ Complete compilation of feedback is attached an as an appendix to the SIR

☐ **Community Technology Advisory Board (CTAB) Presentation**

Date of presentation: [Respond here,]

Summary of comments:

[Respond here.]

☐ Complete meeting minutes and comments are attached an as an appendix to the SIR

☐ Any letters of feedback by CTAB members are attached as an appendix to the SIR

2.4 What does data and conversations with stakeholders tell you about existing racial inequities that influence people's lives and should be taken into consideration when applying/implementing/using the technology? *(See OCR's RET worksheet here for more information; King County Opportunity Maps are a good resource for information based on geography, race, and income.)*

[Respond to question 2.4here.]

2.5 What are the root causes or factors creating these racial inequities? Mitigation strategies will be addressed in 4.1 and 5.3. *Examples: bias in process; lack of access or barriers; lack of racially inclusive engagement.*

[Respond to question 2.5 here.]

3.0 DETERMINE BENEFIT AND/OR BURDEN

Provide a description of any potential disparate impact of surveillance on civil rights and liberties on communities of color and other marginalized communities. Given what you have learned from data and from stakeholder involvement…

3.1 How will the technology, or use of the technology increase or decrease racial equity? What are potential unintended consequences? What benefits may result? Are the impacts aligned with your department's community outcomes that were defined in 1.0?

[Respond to question 3.1 here.]

3.2 What benefits to the impacted community/demographic may result?

[Respond to question 3.1 here.]

3.3 What are potential unintended consequences (both negative and positive potential impact)?

[Respond to question 3.1 here.]

3.4 Are the impacts aligned with your department's community outcomes that were defined in Step 1.0?

[Respond to question 3.1 here.]

4.0 ADVANCE OPPORTUNITY OR MINIMIZE HARM

Provide a mitigation plan for the impacts described in step 3.

4.1 How will you address the impacts (including unintended consequences) on racial equity? What strategies address immediate impacts? What strategies address root causes of inequity listed in 2.5? How will you partner with stakeholders for long-term positive change? If impacts are not aligned with desired community outcomes for surveillance technology (see 1a), how will you re-align your work?

Program Strategies:

[Respond here.]

Policy Strategies:

[Respond here.]

Partnership Strategies:

[Respond here.]

DRAFT

5.0 EVALUATE, RAISE RACIAL AWARENESS, BE ACCOUNTABLE

The following information must be provided to the CTO, via the Privacy Office, on an annual basis for the purposes of an annual report to the City Council on the equitable use of surveillance technology. For Seattle Police Department, the equity impact assessments may be prepared by the Inspector General for Public Safety.

The following information does not need to be completed in the SIR submitted to Council, unless this is a retroactive review.

5.1 Which neighborhoods were impacted/targeted by the technology over the past year and how many people in each neighborhood were impacted?

- ☐ All Seattle neighborhoods
- ☐ Ballard
- ☐ North
- ☐ NE
- ☐ Central
- ☐ Lake Union
- ☐ Southwest
- ☐ Southeast
- ☐ Greater Duwamish
- ☐ East District
- ☐ King County (outside Seattle)
- ☐ Outside King County. Please describe:

[Respond here, if applicable.]

5.2 Demographic information of people impacted/targeted by the technology over the past year…

To the best of the department's ability, provide demographic information of the persons surveilled by this technology. If any of the neighborhoods above were included, compare the surveilled demographics to the neighborhood averages and City averages.

[Respond to question 5.2 here.]

5.3 Which of the mitigation strategies that you identified in Step 4 were implemented in the past year? Specifically, what adjustments to laws and policies should be made to remedy any disproportionate impacts so as to achieve a more equitable outcome in the future.

Type of Strategy (program, policy, partnership)	**Description of Strategy**	**Percent complete of implementation**	**Describe successes and challenges with strategy implementation**

5.4 How have you involved stakeholders since the implementation/application of the technology began?

☐ Public Meeting(s)
☐ CTAB Presentation
☐ Postings to Privacy webpage seattle.gov/privacy
☐ Other external communications
☐ Stakeholders have not been involved since the implementation/application

5.5 What is unresolved? What resources/partnerships do you still need to make changes?

[Respond to question 5.5 here.]

6.0 REPORT BACK

Responses to Step 5 will be compiled and analyzed as part of the CTO's Annual Report on Equitable Use of Surveillance Technology.

Departments will be responsible for sharing their own evaluations with department leadership, Change Team Leads, and community leaders identified in the public outreach plan (Step 2c).

DRAFT

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:

> "*[P]rovide 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

[Assessment to be placed here.]

DRAFT

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.

Neology Back Office System Software (BOSS): System through which ALPR 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.

Neology PIPS: Mobile license plate recognitions system installed in eleven Patrol vehicles.

OCR: "Office of Arts and Culture."

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.

DRAFT

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.

TESU: "Technical and Electronic Support Unit"

Workforce Equity: (Taken from the Racial Equity Toolkit.) Ensure the City's workforce diversity reflects the diversity of Seattle.

DRAFT

APPENDIX B: PUBLIC COMMENT DEMOGRAPHICS AND OVERVIEW

APPENDIX C: PUBLIC MEETING NOTICE(S)

APPENDIX D: MEETING SIGN-IN SHEET(S)

APPENDIX E: MEETING TRANSCRIPT(S)

APPENDIX F: LETTERS FROM ORGANIZATIONS

APPENDIX H: EMAILS FROM THE PUBLIC

APPENDIX I: LETTERS FROM THE PUBLIC

DRAFT