2019 Surveillance Impact Report

CopLogic

Seattle Police Department

Table of Contents

Surveillance Impact Report ("SIR") overview 3

Privacy Impact Assessment 4

Financial Information 23

Expertise and References 25

Racial Equity Toolkit ("RET") and Engagement for Public Comment Worksheet 26

Privacy and Civil Liberties Assessment 35

Submitting Department Memo 36

Appendix A: Glossary 37

Appendix B: Public Comment Analysis 39

Appendix C: Public Comment Demographics 39

Appendix D: Comment Analysis Methodology 39

Appendix E: Questions and Department Responses 39

Appendix F: Public Outreach Overview 39

Appendix G: Meeting Notice(s) 39

Appendix H: Meeting Sign-in Sheet(s) 39

Appendix I: All Comments Received from Members of the Public 39

Appendix J: Letters from Organizations or Commissions 39

Appendix K: Supporting Policy Documentation 40

Appendix L: CTO Notification of Surveillance Technology 47

Surveillance Impact Report ("SIR") overview

About the Surveillance Ordinance

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

How this Document is Completed

This document is completed by the requesting department staff, support and coordinated by the Seattle information technology department ("Seattle it"). As Seattle it and department staff complete the document, they should keep the following in mind.

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

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

Surveillance Ordinance Review Process

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

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

1.0 Abstract

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

CopLogic is crime reporting tool that allows individuals to submit police reports online. SPD utilizes this technology for two purposes: (1) community members may report specific low-level, non-emergency crimes that have occurred within the Seattle city limits, in which there are no known suspects or additional information that would allow for investigation of the crime; and (2) retail businesses that participate in SPD's Retail Theft Program may report low-level thefts that occur in their businesses when they have identified a suspect. CopLogic provides efficient customer service to community members who may need proof of police reporting (i.e., for insurance purposes) without needing to call 9-1-1 then waiting for an officer to respond and take a report. CopLogic frees resources in the 9-1-1 Center, ensuring that 9-1-1 call takers are available for more serious incidents and frees patrol officer resources by eliminating the need for a police officer to be dispatched for the sole purpose of taking a police report.

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

CopLogic is an opt-in system; it is used only when an individual chooses to utilize it. However, individuals may enter personally-identifying information about third parties without providing notice to those individuals, and there is no immediate, systemic method to verify the accuracy of information that individuals provide about those third parties.

2.0 Project / Technology Overview

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

2.1 Describe the benefits of the project/technology.

CopLogic has two tracks:

1) An online public interface allows individuals to report a crime in which no known suspect is available, and for which individuals may need proof of police reporting (i.e., for insurance purposes), without waiting for an officer to dispatch and take a report.
2) An online password-protected interface allows retailers to enter information about retail theft on their property in which a suspect known and suspect information is available.

CopLogic allows for the user, either an individual or a retail store, to report crimes at their own convenience. CopLogic is available 24 hours per day, seven days per week. When users decide that they do not need a police officer to respond to the scene, they may still reap the benefits of reporting an incident, for instance, obtaining a case number for insurance purposes or requesting criminal charges for a theft in their business. CopLogic also eliminates the need for individuals to call 9-1-1 to report a crime and have a report taken. Last year, 14,356 crimes were reported via CopLogic which is 14,356 fewer 9-1-1 calls taken by the 9-1-1 Center. This technology frees resources in the 9-1-1 Center, ensuring that 9-1-1 call takers are available for more serious incidents.

2.2 Provide any data or research demonstrating anticipated benefits.

Research Studies:

- Loss Prevention Technology Case Study *"Using Technology to Enhance the Relationship between Loss Prevention and Local Law Enforcement"*
- Travis Taniguchi and Christopher Salvatore, "Citizen Perceptions of Online Crime Reporting Systems," *The Police Chief* 82 (June 2015): 48–52. http://www.policechiefmagazine.org/citizen-perceptions-of-online-crime-reporting-systems/?ref=3e3a108ad4f36c878bb398b470385dcc

Research shows that allowing individuals to report certain non-urgent crimes and for trained retail loss prevention employees to streamline the shoplifting reporting process provided through online tools such as CopLogic delivers benefits to both the department by eliminating the need for patrol officers to respond in person to take such reports, and providing community members with a secure, convenient, and timely way to interact with police.

SPD has collected data about CopLogic's effectiveness since 2012. The use of CopLogic has increased each year, and it saves numerous police hours by eliminating the need for a patrol officer to respond. The data shows:

	Reports	Hours Saved	Money Saved
2012	7,652	11,478	$573,900.00
2013	9,527	14,290	$714,525.00
2014	12,575	18,862	$943,125.00
2015	12,365	18,547	$927,375.00
2016	13,379	20,068	$1,003,425.00
2017	14,356	21,534	$1,076,700.00
2018*	13,571	20,356	$1,017,825.00

*(2018 Data is calculated through the end of October.)

2.3 Describe the technology involved.

CopLogic is a Software as a Service (SaaS) owned and maintained by LexisNexis. It is used in two ways:

1) Public Interface: Individuals wishing to file a report visit Seattle Police Department's Online Reporting page (https://www.seattle.gov/police/need-help/online-reporting) and follow the prompts to enter information about low-level, non-emergency crimes for which no known suspects exist. CopLogic then generates a report and the reporter receives a temporary unique identification number. An SPD employee, the reviewer, verifies that the report is sufficient and complete. If further information or clarification is needed, the reviewer generates a generic email to the reporter, informing them that the report is missing information that must be included before the file is officially submitted, and providing a link to follow for updates. Once a reviewer determines that the report is complete, the information is electronically transferred into SPD's records management system and receives a general offense (GO) number. This GO number is then provided to the reporter for their records and for insurance purposes.
2) Retail Theft Interface: Retailers who participate in the Seattle Police Department's Retail Theft Program and wish to report a theft first contact the Seattle Police Department's non-emergency number to receive a case number. Then, they access the Retail Theft online page with unique password-protected login information and fill out the Retail Theft online report, which includes information about the retailer, the theft, and the suspect. In most circumstances, retailer security has detained the suspect and included copies of identification with the report that they then submit online.

After a report is made into the Public Interface or the Retail Theft Interface, police officers assigned to the Internet and Telephone Reporting Unit (I-TRU) log in to the CopLogic web portal, utilizing individual user log-in IDs, to access the submitted reports. Once the report is screened by an officer in the I-TRU unit, SPD utilizes an integration server to transfer reports generated in the CopLogic tool into SPD's Records Management System.

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

SPD's mission is to prevent crime, enforce the law, and support quality public safety by delivering respectful, professional, and dependable police services. CopLogic allows for the user, either an individual or a retail store, to report crimes at their own convenience. CopLogic is available 24 hours per day, seven days per week. When users decide that they do not need a police officer to respond to the scene, they may still benefit from reporting an incident, for instance, by quickly obtaining a case number for insurance purposes or requesting criminal charges for a theft in their business. CopLogic also eliminates the need for individuals to call 9-1-1 to report a crime and have a report taken. Last year, 14,356 crimes were reported via CopLogic which is 14,356 fewer 9-1-1 calls taken by the 9-1-1 Center. This technology frees resources in the 9-1-1 Center, ensuring that 9-1-1 call takers, and then patrol officers, are available for more serious incidents.

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

SPD reviewers within the I-TRU unit have access to the reports for the purposes of verifying accuracy and initiating the process of transferring the approved reports into the records management system with a case number (as is assigned to all SPD reports).

Additionally, Seattle IT provides client services and operational support for IT technologies and applications. In supporting SPD systems, operational and application services deploy and service SPD technology systems. Details about the IT department are found in the appendix of this SIR.

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.

CopLogic is used by the public, including retailers, and, thus, its use is triggered whenever an individual instigates the submission of an online report. The SPD reviewer checks the submission for completion and does one of the following:

1) Sends a generic email to the submitter asking for additional information; or
2) Pushes the report to SPD's records management system, providing the report a General Offense ("GO") number, which is then sent back to the submitter.

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

Individuals may use CopLogic to report a crime online when:

1) The crime is within one of these categories of crime:
   a. Property crimes including property destruction, graffiti, car break ins, theft of auto accessories, theft, shoplifting; or
   b. Drug activity, harassing phone calls, credit card fraud, wage theft, identity theft, or lost property
2) The situation is non-emergent
3) The crime occurred within Seattle city limits (exception for identity theft); and
4) No known suspects or information about the crime would allow for additional investigation.

Retailers may use CopLogic to report a retail theft on their property when:

1) The retailer participates in SPD's Retail Theft Program and has obtained a unique login identifier and password;
2) They have detained the suspect;
3) The suspect does not have any outstanding warrants; and
4) They verify the identification of the suspect and upload copies of the suspect's identification, if available.

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.

Only authorized SPD users can access the system, technology, or the data. Access to the application is limited to SPD personnel via password-protected login credentials.

Once data is input by individuals and retail users of CopLogic on the public-facing website, it is accessed and used on SPD's password-protected network.

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.

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.

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.

ITD client services interaction with SPD systems is governed according to the terms of the 2018 Management Control Agreement (MCA) between ITD and SPD, which states that:

"Pursuant to Seattle Municipal Code (SMC) 3.23, ITD provides information technology systems, services and support to SPD and is therefore required to support, enable, enforce and comply with SPD policy requirements." This MCA document may be found in Appendix K.

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.

No information is collected from a source other than the individual instigating the submission of a report.

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

Before anyone is permitted to file a report online, they are prompted to answer a series of questions to determine if online reporting is appropriate for the event they wish to report. In addition, the Seattle Police Department provides guidelines to individuals reporting an event about what information they will need to submit to file a report online. Finally, an authorized SPD employee reviews each submission before accepting the report to ensure that appropriate and adequate information has been provided.

Retail security collects only information that is necessary to document and investigate the crime as required on the Retail Theft Reporting form. No other information is requested.

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?

CopLogic is an online portal that is available for individuals to utilize at any time. It was implemented in the fall of 2011.

Retailers have access to a Retail Theft portal with unique password-protected login information.

CopLogic is a Software as a Service. It utilizes server integration so reports can be transferred to SPD's Records Management System.

4.4 How often will the technology be in operation?

The online portal is continuously in operation, so individuals can instigate and submit reports at any time.

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

CopLogic is a permanent installation.

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?

CopLogic is an online portal, not a physical object. As such, the portal is visible to the public when they visit the online page (https://www.seattle.gov/police/need-help/online-reporting), but is not otherwise visible. The online page contains City of Seattle and SPD branding and contact information. There is also specific text on the web page letting the public know what kind of crimes they may report using this technology.

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

Only authorized SPD users can access the system, technology, or the data. Access to the application is limited to SPD personnel via password-protected login credentials.

Collected data is securely viewed on SPD's password-protected network with access limited to authorized detectives and identified supervisory personnel within the I-TRU unit. Once a reported incident has been reviewed by SPD personnel, it is electronically transferred into the SPD records management system.

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.

Incidental data access may occur through delivery of technology client services. All ITD employees are required to comply with appropriate regulatory requirements regarding security and background review. Information on the ITD roles that may be associated with client services for City Departments can be found in Appendix K.

ITD client services interaction with SPD systems is governed by the terms of the 2018 Management Control Agreement (MCA) between ITD and SPD. The MCA document may be found in Appendix K.

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

CopLogic is owned and maintained by Lexis Nexis. There are no data sharing agreements between SPD and any other entities for CopLogic data. Further, the contract between the City and LexisNexis provides that LexisNexis may only "use, transmit, distribute, modify, reproduce, display, and store the City Data solely for the purposes of (i) providing the Services as contemplated in [its contract with the City]; and (ii) enforcing its rights under [the contract]." A link to the LexisNexis privacy policy can be found here: https://risk.lexisnexis.com/privacy-policy

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

SPD reviewers must access the reports to check for accuracy and approve reports so that the report can be transferred into SPD's records management system with an appropriately assigned case number. Once the information is entered into the records management system, the information can be accessed by authorized SPD personnel at any time, as it relates to a specific investigation, just as is the case with any information stored within the records management system.

Incidental data access may occur through delivery of technology client services. All ITD employees are required to comply with appropriate regulatory requirements regarding security and background review. Information on the ITD roles associated with client services for City Departments can be found in Appendix K.

ITD client services interaction with SPD systems is governed according to the terms of the 2018 Management Control Agreement between ITD and SPD, which states that:

"Pursuant to Seattle Municipal Code (SMC) 3.23, ITD provides information technology systems, services and support to SPD and is therefore required to support, enable, enforce and comply with SPD policy requirements, including the FBIs Criminal Justice Information Services, (CJIS) Security Policy."

The MCA document may be found in Appendix K.

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.)?

CopLogic data is stored remotely and managed by the technology provider, Lexis Nexis. Lexis Nexis is Privacy Shield Certified and adheres to the RELX Group Privacy Shield Principles. Per Lexis Nexis: "We use a variety of administrative, physical and technical security measures to help safeguard your personal information." Additionally, SPD's contract with Lexis Nexis includes a clause for audit, in which the "Consultant shall permit the City and any other governmental agency funding the Work, to inspect and audit all pertinent books and records."

SPD personnel can only access CopLogic data when authorized and provided a username and password for the system. CopLogic creates an audit log that records all activity in the system with usernames and timestamps.

ITD client services interaction with SPD systems is governed according to the terms of the 2018 Management Control Agreement between ITD and SPD, which states that:

"Pursuant to Seattle Municipal Code (SMC) 3.23, ITD provides information technology systems, services and support to SPD and is therefore required to support, enable, enforce and comply with SPD policy requirements, including the FBIs Criminal Justice Information Services, (CJIS) Security Policy."

The MCA document may be found in Appendix K.

5.0 Data Storage, Retention and Deletion

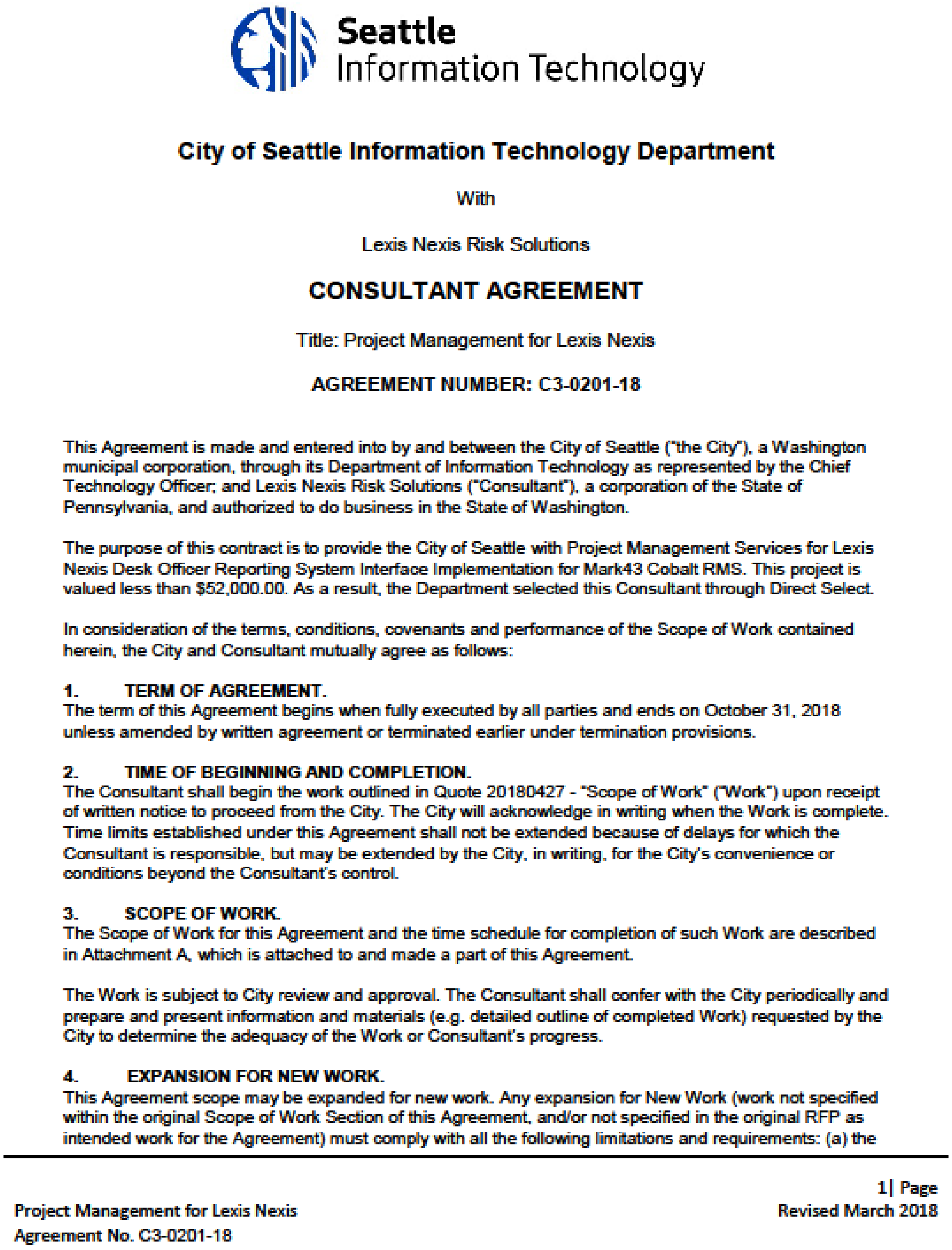
5.1 How will data be securely stored?

CopLogic is a web-hosted solution provided by Lexis Nexis and all information entered into the system is stored on the LexisNexis platform. Per Lexis Nexis: "We use a variety of administrative, physical and technical security measures to help safeguard your personal information." Additionally, Lexis Nexis is Privacy Shield Certified and adheres to the RELX Group Privacy Shield Principles.

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

SPD's Audit, Policy and Research Section (APRS) 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 can audit for compliance at any time.

Additionally, SPD's contract with Lexis Nexis includes a clause for audit, in which the "Consultant shall permit the City and any other governmental agency funding the Work, to inspect and audit all pertinent books and records."



Seattle
Information Technology

City of Seattle Information Technology Department

With

Lexis Nexis Risk Solutions

CONSULTANT AGREEMENT

Title: Project Management for Lexis Nexis

AGREEMENT NUMBER: C3-0201-18

This Agreement is made and entered into by and between the City of Seattle ("the City"), a Washington municipal corporation, through its Department of Information Technology as represented by the Chief Technology Officer; and Lexis Nexis Risk Solutions ("Consultant"), a corporation of the State of Pennsylvania, and authorized to do business in the State of Washington.

The purpose of this contract is to provide the City of Seattle with Project Management Services for Lexis Nexis Desk Officer Reporting System Interface Implementation for Mark43 Cobalt RMS. This project is valued less than $52,000.00. As a result, the Department selected this Consultant through Direct Select.

In consideration of the terms, conditions, covenants and performance of the Scope of Work contained herein, the City and Consultant mutually agree as follows:

1. TERM OF AGREEMENT.
The term of this Agreement begins when fully executed by all parties and ends on October 31, 2018 unless amended by written agreement or terminated earlier under termination provisions.

2. TIME OF BEGINNING AND COMPLETION.
The Consultant shall begin the work outlined in Quote 20180427 - "Scope of Work" ("Work") upon receipt of written notice to proceed from the City. The City will acknowledge in writing when the Work is complete. Time limits established under this Agreement shall not be extended because of delays for which the Consultant is responsible, but may be extended by the City, in writing, for the City's convenience or conditions beyond the Consultant's control.

3. SCOPE OF WORK.
The Scope of Work for this Agreement and the time schedule for completion of such Work are described in Attachment A, which is attached to and made a part of this Agreement.

The Work is subject to City review and approval. The Consultant shall confer with the City periodically and prepare and present information and materials (e.g. detailed outline of completed Work) requested by the City to determine the adequacy of the Work or Consultant's progress.

4. EXPANSION FOR NEW WORK.
This Agreement scope may be expanded for new work. Any expansion for New Work (work not specified within the original Scope of Work Section of this Agreement, and/or not specified in the original RFP as intended work for the Agreement) must comply with all the following limitations and requirements: (a) the

1| Page
Revised March 2018

Project Management for Lexis Nexis
Agreement No. C3-0201-18

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

SPD policy contains multiple provisions to avoid improperly collecting data. SPD Policy 7.010 governs the submission of evidence and requires that all collected evidence be documented in a GO Report. SPD Policy 7.090 specifically governs the collection and submission of photographic evidence. Evidence is submitted to the Evidence Unit and associated with a specific GO Number and investigation. And, SPD Policy 7.110 governs the collection and submission of audio recorded statements. It requires that officers state their name, the Department name, the General Offense number, date and time of recording, the name of the interviewee, and all persons present at the beginning of the recording.

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

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

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

Unit supervisors are responsible for ensuring compliance with data retention requirements within SPD. Audit, Policy & Research Section 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.

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 CopLogic. No person, outside of SPD, has direct access to the application or the data and all requests for information from CopLogic are processed based on existing SPD policies, legal guidelines, and as required by law.

As Seattle IT supports the CopLogic system on behalf of SPD, a Management Control Agreement exists between SPD and Seattle IT. The agreement outlines the specifications for compliance, and enforcement related to supporting the CopLogic system through inter-departmental partnership. The MCA can be found in the appendices of this SIR.

Discrete pieces of information 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 information collected by CopLogic 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 system.

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 system.

6.2 Why is data sharing necessary?

Data sharing is not an automatic component of CopLogic reporting. Instead, discrete pieces of information gleaned from the reports are shared only within the context of the situations outlined in 6.1.

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

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

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

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.

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

The CopLogic system does not automatically check for accuracy. Instead, a reviewer from the I-TRU unit ensures that all fields are completed appropriately by those submitting the report before assigning a General Offense number and approving the report. If necessary information has not been included, the reviewer will contact the reporting party to obtain additional information before the data is electronically transferred into SPD's record management system.

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

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

7.0 Legal Obligations, Risks and Compliance

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

SPD's use of CopLogic is governed by legal requirements and policies as outlined in 3.1, 3.2, 3.3, 4.2, 4.6, and 5.3 of this SIR.

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

SPD Policy 12.050 mandates that all 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.

Privacy risks may arise when information is collected about citizens, unrelated to a specific incident. These concerns are mitigated by the requirement that 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.

CopLogic is to be utilized under specific circumstances, as outlined in 3.2 above. Each report is reviewed to ensure both the accuracy of the report, as well as that it meets the requirements of online reporting (again, as outlined in 3.2 above).

Additionally, SMC 14.12 and SPD Policy 6.060 direct all SPD personnel that "any documentation of information concerning a person's sexual preferences or practices, or their political or religious activities must be for a relevant reason and serve a legitimate law enforcement purpose." Additionally, officers must take care "when photographing demonstrations or other lawful political activities. If demonstrators are not acting unlawfully, police can't photograph them."

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.

Finally, see 5.3 for a detailed discussion about procedures related to noncompliance.

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?

The privacy risks outlined in 7.3 above are mitigated by legal requirements and auditing processes that allow for any auditor, including the Office of Inspector General and the federal monitor, to inspect use and deployment of CopLogic.

The largest privacy risk is the un-authorized release of reported information deemed private or offensive in the RCW. To mitigate this risk, the technology falls under the current SPD policies around dissemination of Department data and information reflected in 6.1.

8.0 Monitoring and Enforcement

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

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 subpoenas and requests for public disclosure are logged by SPD’s Legal Unit. Any action taken, and data released subsequently in response to subpoenas is then tracked through a log maintained by the Legal Unit. Public disclosure requests are tracked through the City’s GovQA Public Records Response System, and 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.

SPD’s Audit, Policy and Research Section is authorized to conduct audits of all investigative data collection software and systems. In addition, the Office of Inspector General and the federal monitor can conduct audits of the software, and its use, at any time. Audit data is available to the public via Public Records Request.

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
2010	2010	$33,000	N/A	N/A	SPD Budget

Notes:

N/A

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
$10,365	N/A	N/A	N/A	SPD Budget

Notes:

2018 Cost (after-tax) per the Contracts Renewal Log

1.3 Cost savings potential through use of the technology

SPD has collected data about CopLogic's effectiveness since 2012. The use of CopLogic has increased each year, and it saves numerous police hours. The data shows:

	Reports	Hours Saved	Money Saved
2012	7,652	11,478	$573,900.00
2013	9,527	14,290	$714,525.00
2014	12,575	18,862	$943,125.00
2015	12,365	18,547	$927,375.00
2016	13,379	20,068	$1,003,425.00
2017	14,356	21,534	$1,076,700.00
2018*	13,571	20,356	$1,017,825.00

*(2018 Data is calculated through the end of October.)

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

This question is not applicable.

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
King County Sheriff's Office	King County Sheriff's Office Communications Center Phone: (206) 296-3311 Fax: (206) 205-7956	King County uses CopLogic similarly to SPD, allowing the public to report specific non-emergency crimes to the Sheriff's Office.

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
N/A	N/A	N/A

3.0 White Papers or Other Documents

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

Title	Publication	Link
Using Technology to Enhance the Relationship between Loss Prevention and Local Law Enforcement	Loss Prevention Magazine. (Sept-Oct. 2015)	LPPORTAL.COM
Citizen Perceptions of Online Crime Reporting Systems	*The Police Chief* 82 (June 2015): 48–52.	http://www.policechiefmagazine.org/citizen-perceptions-of-online-crime-reporting-systems/?ref=3e3a108ad4f36c878bb398b470385dcc

Racial Equity Toolkit ("RET") and Engagement for Public Comment Worksheet

Purpose

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

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

Adaptation of the RET for Surveillance Impact Reports

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

Racial Equity Toolkit Overview

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

1.0 Set Outcomes

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

☐ The technology disparately impacts disadvantaged groups.

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

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

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

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

The potential impacts of this system on civil liberties are minimal. The risk with this technology is that this information could be disseminated for use in ways that could negatively impact peoples' civil liberties. CopLogic is an opt-in system; it is used only when an individual chooses to utilize it. However, individuals may enter personally-identifying information about third parties without providing notice to those individuals, and there is no immediate, systemic method to verify the accuracy of information that individuals provide about those third parties.

Data entered into CopLogic is reviewed by trained SPD 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.

Additionally, SPD has established policies regarding the dissemination of data in connection with criminal prosecutions, Washington Public Records Act (Chapter 42.56 RCW), and other data sharing.

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.

Because the information received through the CopLogic portal comes from community members there is a risk that racial or ethnicity-based biased information may be entered. All the information entered is screened by authorized and trained SPD personnel. 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.

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.

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

☒ all Seattle neighborhoods

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County.

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

N/A

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

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%.

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?

This technology is web-based and available for use by anyone within the city of Seattle with access to the internet, including mobile devices.

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?

The Aspen Institute on Community Change defines *structural racism* as "…public policies, institutional practices, cultural representations and other norms [which] work in various, often reinforcing ways to perpetuate racial group inequity."[1] 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.

No person outside of SPD has direct access to the CopLogic data. Data obtained by the system may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law. See section 6.0 for more details about data sharing.

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?

Like decisions around data sharing, data storage and retention have similar potential for disparate impact on historically targeted communities. Because the use of this technology is an opt-in decision by its community users, the risks of improper or biased usage are limited. All information, once reviewed by authorized SPD employees, is electronically transferred into SPD's records management system. The SPD employees tasked with this review are bound by SPD policies pertaining to electronic communications, computer and data usage, and bias-based policing.

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

The potential unintended consequences include individuals using the CopLogic system incorrectly in attempt to contact SPD (for example: when an emergency response is appropriate), and the dissemination of information through negligence or misconduct (intentional and unintentional). These are mitigated by documentation and function within the public website portal, review of entered information by SPD personnel, and the application of existing SPD policy.

[1] Aspen Institue Roundtable on Community Change. 2008. "Dismantling Structural Racism: A Racial Equity Theory of Change." Washington D.C.: The Aspen Institute.

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. ACLU of Washington	2. Ethiopian Community Center	3. Planned Parenthood Votes Northwest and Hawaii
4. ACRS (Asian Counselling and Referral Service)	5. Faith Action Network	6. PROVAIL
7. API Chaya	8. Filipino Advisory Council (SPD)	9. Real Change
10. API Coalition of King County	11. Friends of Little Saigon	12. SCIPDA
13. API Coalition of Pierce County	14. Full Life Care	15. Seattle Japanese American Citizens League (JACL)
16. CAIR	17. Garinagu HounGua	18. Seattle Neighborhood Group
19. CARE	20. Helping Link	21. Senior Center of West Seattle
22. Central International District Business Improvement District	23. Horn of Africa	24. Seniors in Action
25. Church Council of Greater Seattle	26. International ImCDA	27. Somali Family Safety Task Force
28. City of Seattle Community Police Commission (CPC)	29. John T. Williams Organizing Committee	30. South East Effective Development
31. City of Seattle Community Technology Advisory Board	32. Kin On Community Health Care	33. South Park Information and Resource Center SPIARC
34. City of Seattle Human Rights Commission	35. Korean Advisory Council (SPD)	36. STEMPaths Innovation Network
37. Coalition for Refugees from Burma	38. Latina/o Bar Association of Washington	39. University of Washington Women's Center
40. Community Passageways	41. Latino Civic Alliance	42. United Indians of All Tribes Foundation
43. Council of American Islamic Relations - Washington	44. LELO (Legacy of Equality, Leadership, and Organizing)	45. Urban League
46. East African Advisory Council (SPD)	47. Literacy Source	48. Wallingford Boys & Girls Club
49. East African Community Services	50. Millionair Club Charity	51. Washington Association of Criminal Defense Lawyers
52. Education for All	53. Native American Advisory Council (SPD)	54. Washington Hall
55. El Centro de la Raza	56. Northwest Immigrant Rights Project	57. West African Community Council
58. Entre Hermanos	59. OneAmerica	60. YouthCare
61. US Transportation expertise	62. Local 27	63. Local 2898
64. (SPD) Demographic Advisory Council	65. South Seattle Crime Prevention Coalition (SSCPC)	66. CWAC
67. NAAC		

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	**Updated 2/12/19:** Bertha Knight Landes Room, 1st Floor City Hall 600 4th Avenue, Seattle, WA 98104
Time	February 27, 2019; 6:00 p.m. – 8:00 p.m.
Capacity	100+
Link to URL Invite	Not Available

2.2 Scheduled Focus Group Meeting(s)

Meeting 1

Community Engaged	
Date	

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].

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

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

5.0 Equity Annual Reporting

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

Respond here.

Privacy and Civil Liberties Assessment

Purpose

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

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

Working Group Privacy and Civil Liberties Assessment

Respond here.

Submitting Department Memo

Description

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

Purpose

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

Benefits to the Public

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

Privacy and Civil Liberties Considerations

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

Summary

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

Appendix A: Glossary

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

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

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

DON: “department of neighborhoods.”

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

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

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

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

OCR: “Office of Civil Rights.”

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

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

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

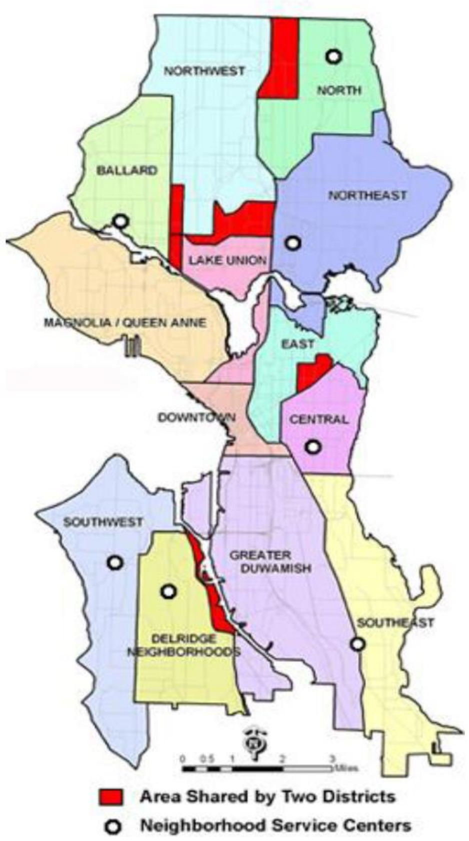
RET: "racial equity toolkit"

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

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

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

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



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

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

Appendix B: 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

Management Control Agreement

Management Control Agreement Between
Seattle Police Department and
City of Seattle Information Technology Department

The City of Seattle Police Department ("SPD"), also referred to as the Criminal Justice Agency, and the City of seattle Information Technology Department (''ITD") are departments of the municipal corporation of the City of Seattle.

Pursuant to Seattle Municipal Code ("SMC") 3.23, ITD provides information technology systems, services, and support to SPD and is therefore required to support, enable, enforce, and comply with SPD policy requirements, including the FBI's Criminal Justice Information Services ("CJIS") Security Policy.

Pursuant to the CJIS Security Policy, it is agreed that with respect to the administration of computer systems, network infrastructure, devices, and services interfacing directly or indirectly with A Central Computerized Enforcement System ("ACCESS") for the exchange of criminal history/criminal justice information, the Criminal Justice Agency shall have the authority, via managed control, to set and enforce:

Priorities that guarantee the priority, integrity, and availability of service needed by the criminal justice community.

Requirements for the selection, authorization, supervision, and termination of physical and logical access to Criminal Justice Information ("CJI").

Policy governing operation of justice systems, data, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a communications network and related criminal justice systems to include but not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.

Restriction of unauthorized physical and logical access to or use of systems and equipment accessing CJI.

Compliance with all rules and regulations of the Criminal Justice Agency policies and CJIS Security Policy in the operation of, access to, or control over any CJI systems, data, or infrastructure.

The responsibility for management control of the criminal justice function remains solely with the Criminal Justice Agency. ITD will not enter into any agreements or allow any access to, possession of, or control over any SPD CJI systems, data, or infrastructure

without explicit authorization from at least one SPD Authorized Party. SPD Authorized Parties must be SPD employees and include:
Chief of Police
Chief Operating Officer

This agreement covers the overall supervision of all Criminal Justice Agency systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, administration, and maintenance of any Criminal Justice Agency system to include NCIC Programs that may be subsequently designed and/or implemented within the Criminal Justice Agency.

Additional agreements, such as a Memorandum of Agreements, Service Level Agreements, and/or Continuity Plans, may be established and maintained to further delineate, define, and assign roles, responsibilities, and requirements of and agreements between SPD and ITD, and other City of Seattle Departments and/or agencies.

Tracye Cantrell

Tracye Cantrell
Interim Chief Technology Officer
Seattle Information Technology Department

Date Feb 2, 2018

Carmen Best

Carmen Best
Interim Chief of Police |
Seattle Police Department

Date 2-7-2018

Reference: CJIS Security Policy, Version 5.5, dated June 1, 2016 (CJISD-ITS-DOC-08140-5 .5)

IT Support Services for City Technology

Engineering and Operations

This division designs, implements, operates, and supports technology solutions and resources in accordance with city wide architecture and governance. Responsibilities for this division include:

- Primary communications networks that provide public safety and constituent access to and from City government; the telephone system, the data network, and Public Safety Radio System. Responsible for sustaining all three systems operating as close to 100% availability as possible 24 hours a day, seven days a week.
- Design, acquisition, installation, maintenance, repair and management of fiber optic cables on behalf of City departments and approximately 20 other local, state and federal agencies.
- Procurement requests, allocation, operation and maintenance of city wide and departmental servers, virtual enterprise computing and SAN storage environments for large scale mission critical applications in a secure, reliable, 24/7 production environment for enterprise computing.
- Allocation, operation and maintenance of enterprise level services like messaging services, web access, file sharing, user management and remote access solutions.
- Collaborate with Enterprise Architecture team to develop standards for information technology equipment and software.
- Service Desk and technical support services for City's computers, peripherals, electronic devices and mobile device management.
- Centralized IT asset management to include research, procurement request, surplus and asset transfer.
- Facility management for a reliable production computing environment to the City departments.
- Support for other enterprise services and tools.

Compute System Technologies

This team manages the operations and maintenance of computing infrastructure, including servers, storage, backup and recovery, and enterprise support systems (e.g., Active Directory, VPN, etc.). The team is also responsible for safeguarding systems and data by performing required security patches, updates, and backups to ensure systems operate at as close to 100% availability as possible 24x7. Units within this group include:

Systems Operations. The team is focused on delivering the computing environment across multiple departments. The team has technical expertise to design, integrate, and operate a secure, reliable computing environment. Key technologies include Windows, Solaris, IBM AIX, and Linux.

Enterprise Services. Enterprise Services (ES) are large scale infrastructure and application services used by the City of Seattle end user community. This includes both SaaS and NGDC hosted infrastructure and application services. The team is responsible for EA vendor management, system administration, upgrades and technical support. Key technologies includes Microsoft Active Directory (AD), Distributed File System (DFS), Exchange Online, Office 365 and SharePoint Online infrastructure.

Infrastructure Tools. The team provides a single focus for the design, planning, deployment and maintenance of standard enterprise infrastructure monitoring and management tools. This includes system performance (Solarwinds, SCOM), configuration management (SCCM, WSUS), and monitoring and system management (Trend Micro, CRM, Vipre).

Virtual and Data Infrastructure. This team engineers and operates reliable, flexible, performant virtualized Windows, UNIX and Linux platforms and their related technologies in direct support of critical business applications. Key technologies include Solaris, Unix, Linux, Windows, and vmWare, and the associated virtualization Nutanix, IBM LPAR, and Solaris hardware.

The team also engineers and operates reliable, flexible, performant storage and data protection solutions to host and protect critical business data of all types, leveraging SAN, NAS, object, and cloud technologies. Key technologies include Dell Compellent, Quantum, Hitachi, NetApp, Cloud storage, Brocade fiber channel switching, and Commvault.

Network And Communications Technologies

This team is responsible for designing, installing, operating, and maintaining data, voice, radio, fiber optic, and structured cabling infrastructure that integrates with other technologies to provide access to resources used by City departments and the public we serve. Units within this group include:

Network Engineering & Operations. The Network Services team engineers, operates and maintains the City's data network, including data center core networks, the internet perimeter, the network backbone, and local area networks that support systems and users across the City. This group designs, acquires, installs, maintains, repairs, and manages an enterprise data network that aligns with City architectures and standards. This group also participates in development of those standards and provides tier 2 and 3 end user support. This team supports technologies that include routing, switching, load balancing, enterprise Wi-Fi, DNS/DHCP/NTP, and network security (including firewalls, VPN appliances, certificate infrastructure, network access control, and web filtering.)

Telecommunication Engineering & Operations. The Telecommunications Services team engineers, operates, and maintains a highly-reliable enterprise telephone and contact center infrastructure. This group supports end user move and change activity and provides tier 2 and 3 support. The Telecommunication Services team acquires, installs, maintains, and repairs telecommunications equipment and manages commercial telephony circuits. It supports technologies that include VoIP, circuit-switched telephony, voice mail, contact center services (including call routing scripts), audio conference bridges, commercial telephony services, SONET, and WDM.

Radio & Communications Infrastructure. This team delivers radio services for public safety and other government departments. It provides extremely reliable infrastructure and support for end user mobile and portable radio equipment. The group installs and maintains communications equipment inside 911 dispatch centers and City vehicles, with primary support to SPD and SFD. The team also supports regional planning, maintenance, interoperability testing, and projects (including PSERN and Washington OneNet) in partnership with other local, state, and federal agencies. This team also designs, acquires, installs, maintains, repairs, and manages in-building structured cabling systems and outside plant fiber optic and copper cable infrastructure for the City and approximately 20 external public agency partners. Technologies include trunked and conventional land mobile radio, microwave radio and other wireless communications systems (including point-to-multipoint and mesh networks,) distributed antenna systems, routing/MPLS, DS3/T1/DACS, outside plant cable infrastructure (including fiber and copper,) and structured cabling infrastructure.

End User Support

This team is responsible for providing a single point of contact for IT technical support, trouble ticket and service request resolution and referral services to other IT workgroups, and for communication for all changes, patches, upgrades and standards changes. The team is also responsible for providing technical support for the City's desktop computers, peripherals, electronic devices and mobile devices. Units within this group include:

Service Desk. The Service Desk team provides a single point of contact for Seattle IT services, promptly resolving incidents and service requests when first contacted whenever possible, escalating issues accurately and efficiently, and keeping users and partners aware of service status and changes.

Device Support. This team provides direct customer support for end user computing to all departments within the City and tier 2 escalation support and management of centralized end user computing applications and hardware. requests.

Device Engineering. This team engineers and deploys software packages for end user applications, device drivers, patches, security updates and custom packages as required. This team evaluates and recommends hardware and software for end user standards. In addition, this team provides tier 3 escalation support and management of centralized end user computing applications and hardware.

Asset Management. This team is responsible tracking and inventory controls for city wide IT assets including desktops, laptops, printers, servers, switches, and miscellaneous Information Technology infrastructure. In addition to inventory control, the team will be forecasting replacement cycles for equipment based on City standards to promote a stable computing environment.

IT Operations Support

The IT Operations Support team is responsible for management of Information Technology facilities (including data centers and communications equipment rooms), and installation and cabling equipment within those facilities. This team provides the enterprise Network Operations Center (NOC) that monitors alerts, performs initial incident analysis, dispatches tier 2 and 3 technical support, and provides initial incident communication for network infrastructure and computing systems managed by Engineering and Operations. Units within this group include:

Installation Management. This team installs networking and computing equipment in data centers, communications rooms and wiring closets; installs and maintains network cabling within data centers and equipment rooms according to City standards; and supports repair and end user move and change activity (including telephone move projects).

IT Operations Center. This team manages facilities which support City computing and communications services. This includes managing access to facilities, coordinating vendors, maintaining records (including data center inventory management), and, where applicable, monitoring facility systems (including CRUs, fire alarms, water detection sensors, UPS systems, and power consumption). This team also staffs the NOC that monitors alerts from network infrastructure and computing systems, performs initial problem analysis, dispatches appropriate tier 2 and 3 technical support team(s), and provides initial incident communication.

Application Services

This division designs, develops, integrates, implements, and supports application solutions in accordance with city wide architecture and governance. Its teams are organized to support business functions or service groups**.** The integration of application services will be completed gradually in 2017, with details of the organization and integration process still under development.

Applications

These teams will provide development and support for applications that include customer relationship management, billing, finance, human resources, work and asset management and records management.

Shared Platforms

These teams will provide development and support for applications that include engineering, spatial analysis, business intelligence, analytics, SharePoint Online and document management.

Cross Platform Services

These teams will provide support to application teams, including quality assurance, change control, database administration, integration services, and access management activities.

Appendix L: CTO Notification of Surveillance Technology

Thank you for your department’s efforts to comply with the new Surveillance Ordinance, including a review of your existing technologies to determine which may be subject to the Ordinance. I recognize this was a significant investment of time by your staff; their efforts are helping to build Council and public trust in how the City collects and uses data.

As required by the Ordinance (SMC 14.18.020.D), this is formal notice that the technologies listed below will require review and approval by City Council to remain in use. This list was determined through a process outlined in the Ordinance and was submitted at the end of last year for review to the Mayor's Office and City Council.

The first technology on the list below must be submitted for review by March 31, 2018, with one additional technology submitted for review at the end of each month after that. The City's Privacy Team has been tasked with assisting you and your staff with the completion of this process and has already begun working with your designated department team members to provide direction about the Surveillance Impact Report completion process.

Please let me know if you have any questions.

Thank you,

Michael Mattmiller

Chief Technology Officer

Technology	Description	Proposed Review Order
Automated License Plate Recognition (ALPR)	ALPRs are computer-controlled, high-speed camera systems mounted on parking enforcement or police vehicles that automatically capture an image of license plates that come into view and converts the image of the license plate into alphanumeric data that can be used to locate vehicles reported stolen or otherwise sought for public safety purposes and to enforce parking restrictions.	1
Booking Photo Comparison Software (BPCS)	BCPS is used in situations where a picture of a suspected criminal, such as a burglar or convenience store robber, is taken by a camera. The still screenshot is entered into BPCS, which runs an algorithm to compare it to King County Jail booking photos to identify the person in the picture to further investigate his or her involvement in the crime. Use of BPCS is governed by SPD Manual §12.045.	2
Forward Looking Infrared Real-time video (FLIR)	Two King County Sheriff's Office helicopters with Forward Looking Infrared (FLIR) send a real-time microwave video downlink of ongoing events to commanders and other decision-makers on the ground, facilitating specialized radio tracking equipment to locate bank robbery suspects and provides a platform for aerial photography and digital video of large outdoor locations (e.g., crime scenes and disaster damage, etc.).	3

Technology	Description	Proposed Review Order
Undercover/ Technologies	The following groups of technologies are used to conduct sensitive investigations and should be reviewed together. • **Audio recording devices**: A hidden microphone to audio record individuals without their knowledge. The microphone is either not visible to the subject being recorded or is disguised as another object. Used with search warrant or signed Authorization to Intercept (RCW 9A.73.200). • **Camera systems**: A hidden camera used to record people without their knowledge. The camera is either not visible to the subject being filmed or is disguised as another object. Used with consent, a search warrant (when the area captured by the camera is not in plain view of the public), or with specific and articulable facts that a person has or is about to be engaged in a criminal activity and the camera captures only areas in plain view of the public. • **Tracking devices**: A hidden tracking device carried by a moving vehicle or person that uses the Global Positioning System to determine and track the precise location. U.S. Supreme Court v. Jones mandated that these must have consent or a search warrant to be used.	4
Computer-Aided Dispatch (CAD)	CAD is used to initiate public safety calls for service, dispatch, and to maintain the status of responding resources in the field. It is used by 911 dispatchers as well as by officers using mobile data terminals (MDTs) in the field.	5
CopLogic	System allowing individuals to submit police reports on-line for certain low-level crimes in non-emergency situations where there are no known suspects or information about the crime that can be followed up on. Use is opt-in, but individuals may enter personally-identifying information about third-parties without providing notice to those individuals.	6

Technology	Description	Proposed Review Order
Hostage Negotiation Throw Phone	A set of recording and tracking technologies contained in a phone that is used in hostage negotiation situations to facilitate communications.	7
Remotely Operated Vehicles (ROVs)	These are SPD non-recording ROVs/robots used by Arson/Bomb Unit to safely approach suspected explosives, by Harbor Unit to detect drowning victims, vehicles, or other submerged items, and by SWAT in tactical situations to assess dangerous situations from a safe, remote location.	8
911 Logging Recorder	System providing networked access to the logged telephony and radio voice recordings of the 911 center.	9
Computer, cellphone and mobile device extraction tools	Forensics tool used with consent of phone/device owner or pursuant to a warrant to acquire, decode, and analyze data from smartphones, tablets, portable GPS device, desktop and laptop computers.	10
Video Recording Systems	These systems are to record events that take place in a Blood Alcohol Concentration (BAC) Room, holding cells, interview, lineup, and polygraph rooms recording systems.	11
Washington State Patrol (WSP) Aircraft	Provides statewide aerial enforcement, rapid response, airborne assessments of incidents, and transportation services in support of the Patrol's public safety mission. WSP Aviation currently manages seven aircraft equipped with FLIR cameras. SPD requests support as needed from WSP aircraft.	12
Washington State Patrol (WSP) Drones	WSP has begun using drones for surveying traffic collision sites to expedite incident investigation and facilitate a return to normal traffic flow. SPD may then request assistance documenting crash sites from WSP.	13
Callyo	This software may be installed on an officer’s cell phone to allow them to record the audio from phone communications between law enforcement and suspects. Callyo may be used with consent or search warrant.	14

Technology	Description	Proposed Review Order
I2 iBase	The I2 iBase crime analysis tool allows for configuring, capturing, controlling, analyzing and displaying complex information and relationships in link and entity data. iBase is both a database application, as well as a modeling and analysis tool. It uses data pulled from SPD's existing systems for modeling and analysis.	15
Parking Enforcement Systems	Several applications are linked together to comprise the enforcement system and used with ALPR for issuing parking citations. This is in support of enforcing the Scofflaw Ordinance SMC 11.35.	16
Situational Awareness Cameras Without Recording	Non-recording cameras that allow officers to observe around corners or other areas during tactical operations where officers need to see the situation before entering a building, floor or room. These may be rolled, tossed, lowered or throw into an area, attached to a hand-held pole and extended around a corner or into an area. Smaller cameras may be rolled under a doorway. The cameras contain wireless transmitters that convey images to officers.	17
Crash Data Retrieval	Tool that allows a Collision Reconstructionist investigating vehicle crashes the opportunity to image data stored in the vehicle's airbag control module. This is done for a vehicle that has been in a crash and is used with consent or search warrant.	18
Maltego	An interactive data mining tool that renders graphs for link analysis. The tool is used in online investigations for finding relationships between pieces of information from various sources located on the internet.	19

Please let me know if you have any questions.

Thank you,

Michael