City of Seattle

2021 Surveillance Impact Report

Link Analysis Software - IBM I2 iBase

Seattle Police Department

Surveillance Impact Report ("SIR") overview

About the Surveillance Ordinance

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

How this Document is Completed

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

1. Responses to questions should be in the text or check boxes only; all other information (questions, descriptions, etc.) Should **not** be edited by the department staff completing this document.
2. All content in this report will be available externally to the public. With this in mind, avoid using acronyms, slang, or other terms which may not be well-known to external audiences. Additionally, responses should be written using principally non-technical language to ensure they are accessible to audiences unfamiliar with the topic.

Surveillance Ordinance Review Process

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

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

I2 iBase is the server backbone to the i2 Analysts Notebook application, a software system which organizes existing SPD data visually into more accessible information utilized by the SPD Real Time Crime Center (RTCC) employees. The purpose of the RTCC is to provide actionable information to units in the field to increase officer safety, efficiency, and response to incidents. It is also intended to be the information "hub" of the police department, utilizing its resources and collective knowledge to enhance the department's effectiveness at reducing crime and improving public safety. The iBase system combines data stored in SPD's Records Management System (RMS), Computer Aided Dispatch (CAD) system, and information gathered during criminal investigations and displays information related to ongoing investigations. This type of link analysis software is similar to a virtual "link board" or "pin board", helping investigators to visualize the connections between known entities, vehicles, locations, etc. in the course of a criminal investigation.

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

Prior to the implementation of the iBase software, investigators were required to re-type all criminal information from RMS onto visualization charts, which was a time-consuming and redundant process. Implementing iBase gave users direct access to that information without having to re-type it. This software is used exclusively for ongoing criminal investigations and therefore necessarily includes personal information about subjects of those investigations.

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.

This software prevents investigators from having to re-type RMS information onto a chart. Visualizing criminal information provides investigators a more thorough understanding of complicated criminal investigations.

2.2 Provide any data or research demonstrating anticipated benefits.

Professional police departments have been utilizing manual link analysis in the form of "link boards" or "pin boards" for decades, and "connecting the dots" is a hallmark of investigative practice. In the 1990s Malcom Sparrow first introduced the concept of social network analysis to law enforcement and criminal investigations. Link analysis, a component of social network analysis, is a tool used to identify relationships in data. Though simple link analysis with a limited number of points of data can be charted manually, as the number of pieces of data, or "observations" increases, the processing power of a computer helps the analyst provide a more thorough and complete analysis of the links between the available data. Beyond just demonstrating an association, link analysis frequently is employed in an effort to highlight the relative strength of relationships[1]. These types of analysis techniques in criminal intelligence are used to organize data and reveal patterns in the nature and extent of relationships between data points. They also provide effective visualizations of both qualitative and quantitative data which are valuable in presenting intelligence assessments[2]. An important component of link analysis software is the ability for investigators to identify the significance of new information as it is added [3].

Prior to the implementation of the software, users had to re-type the information associated to a criminal investigation (e.g. Names, Dates of Birth, Criminal Histories) onto a chart if they wished to visualize the case. While no formal study was done of the time wasted on these tasks, adding a single person's criminal history to a chart could take multiple days of work. With this software, a user can see a subject's criminal history in minutes.

[1] McCue, Colleen. (2015). Data Mining and Predictive Analysis (Second Edition).

[2] Strang, Steven. (2014). Network Analysis in Criminal Intelligence.

[3] Burcher, Morgan, and Chad Whelan. (2018). "Social Network Analysis as a Tool for Criminal Intelligence: Understanding Its Potential from the Perspectives of Intelligence Analysts." Trends in Organized Crime 21 (3): 278–94

2.3 Describe the technology involved.

The iBase software is a SQL server that imports a portion of the data from SPD's RMS and CAD systems, allowing users to visualize the data in a link chart (rather than the standard textual display in RMS/CAD). The iBase server is an on-premise security encrypted server housed and managed by Seattle IT meeting CJIS approved requirements. The client i2 Analyst's Notebook software is locally installed on RTCC analysts' workstations. An automated electronic data transfer allows information located within SPD's RMS and CAD systems to be imported into the iBase system via a one-way transfer of data from the source systems to iBase. i2 iBase is a relational database environment for searching through investigation data imported from RMS and CAD as well as manually imported information gathered by investigators during the course of a criminal investigation. IBM i2 Analyst's Notebook is the worldwide standard software solution for operational crime analysis and visualization, with the purpose of creating relevant intelligence from large amounts of data. Various types of structured data are compared and visualized through a variety of heatmaps, relationships, and diagrams.

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

The mission of the Seattle Police Department is to prevent crime, enforce the law, and support quality public safety by delivering respectful, professional, and dependable police services. SPD's department priorities include the use of best practices that include officer safety guidelines and performance-based accountability to provide progressive and responsive police services to crime victims, witnesses, and all members of the community, and to structure the organization to support the SPD mission and field a well-trained sworn and non-sworn workforce that uses technology, training, equipment, and research strategically and effectively. The utilization of the IBM Security i2 iBase system increases efficiency of investigations, availability of data, awareness of situational information, and timeliness of actionable information to officers on the street.

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

Only trained, backgrounded, and CJIS certified employees of SPD's Real Time Crime Center and supporting Seattle IT employees have access to the i2 iBase system and i2 Analyst's Notebook software.

All authorized users of CAD are Criminal Justice Information Services (CJIS) certified and maintain Washington State ACCESS (A Central Computerized Enforcement Service System) certification. More information on CJIS compliance may be found at the CJIS Security Policy website. Additional information about ACCESS may be found on the Washington State Patrol's website.

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.

IBM Security i2 iBase system is only used during the investigation of crimes by the SPD Real Time Crime Center. Access for personnel into the system is predicated on state and federal law governing access to Criminal Justice Information Services (CJIS). This includes pre-access background information, appropriate role-based permissions as governed by the CJIS security policy found in Appendix M, and audit of access and transaction logs within the system. All users of CAD must be CJIS certified and maintain Washington State ACCESS certification.

Each user must be directly granted an account (tied to their SPD network identity) in order to access the software. The software logs: user sign on/off, each time a user accesses any piece of data, and any data manually added by a user. These logs are periodically reviewed to ensure proper use of the software; they may also be reviewed at any time by the Seattle Intelligence Ordinance Auditor.

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

IBM Security i2 iBase system is only used during the investigation of crimes by the SPD Real Time Crime Center and information collected and stored in the system is related to these criminal investigations.

All use of the i2 iBase system must also comply with SPD Policy 12.050 – Criminal Justice Information Systems and may only be used for legitimate criminal investigative purposes.

Use of the iBase system is governed by the City of Seattle Intelligence Ordinance (SMC 14.12), 28 CFR Part 23, CJIS requirements, and any future applicable requirements.

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

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

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.

All authorized users of CAD must be CJIS certified and must maintain Washington State ACCESS certification, and trained directly in the use of the iBase software, in addition to all standard SPD training and Directives.

SPD Policy 12.050 defines the proper use of criminal justice information systems.

Outside of SPD, Seattle Information Technology Department (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, including the FBIs Criminal Justice Information Services, (CJIS) Security Policy."

4.0 Data Collection and Use

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

The only information pulled into iBase automatically comes from SPD's Records Management System (RMS) and Computer Aided Dispatch (CAD) system. Users may manually add additional information that they have collected during the course of a criminal investigation,. All manually added information is deleted after five years, in accordance with 28 CFR Part 23. No data outside SPD's RMS/CAD (e.g. commercial data aggregators, publicly available data, or other city departments) is automatically collected.

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

All data entered into the iBase system is directly related to criminal investigations. Individual detectives and analysts may manually enter information not imported from the existing RMS and CAD data systems. Analysts use this software to build networks of individuals associated with criminal cases.

All data changes are logged in the software's audit log, which is reviewed periodically. In addition, when manually adding information, a user must provide the source description, source reliability, and content certainty; all manually added information is purged from the system after 5 years, in compliance with 28 CFR Part 23.

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?

IBM i2 iBase is currently in use by the RTCC to assist with criminal investigations and to provide actionable information to units in the field. SPD employees in the RTCC and Investigations Unit utilize the i2 Analyst's Notebook software and information stored in the i2 iBase system. It may also be used in compliance with the City of Seattle Intelligence Ordinance.

4.4 How often will the technology be in operation?

The software itself resides on a server that is operational 24/7. Users may access the data at any time, as part of criminal investigations.

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

The software is installed on a server and may be removed at any time. There is no physical installation aspect to this project.

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?

No physical object is collecting any data.

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

Data stored in the i2 iBase system is accessed by SPD employees assigned to the Real Time Crime Center and Investigations Unit. Access to the application requires SPD personnel to log in with password-protected login credentials which are granted to employees with business needs to access CAD. These employees are ACCESS and CJIS certified.

According to the CJIS security policy, "The agency shall configure the application, service, or information system to provide only essential capabilities and shall specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.".

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, 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.

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."

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

No outside agency has direct access to the software.

I2 iBase is operated and used exclusively by SPD personnel. Seattle IT Department personnel have administrative access to the system for support services as outlined in 4.7. Use of the iBase system will be governed by the City of Seattle Intelligence Ordinance, 28 CFR Part 23, CJIS requirements, and any future applicable requirements.

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

I2 iBase is used by the RTCC to assist in ongoing criminal investigations and to provide actionable information to units in the field to increase officer safety, efficiency, and response to incidents. Data is only accessed as part of ongoing criminal investigations or under the City of Seattle Intelligence Ordinance.

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.)?

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. All user activity within the iBase system generates a log that is auditable.

Data is securely input and used on SPD's password-protected network with access limited to authorized users.

The entire system is located on the SPD network that is protect by industry standard firewalls. ITD performs routine monitoring of the SPD network.

The CAD system is CJIS compliant. More information on CJIS compliance may be found at the CJIS Security Policy website.

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.

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 audit for compliance at any time.

ITD client services interaction with SPD systems is governed by the terms of the 2017 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."

5.0 Data Storage, Retention and Deletion

5.1 How will data be securely stored?

All of the data in the iBase system are held in SPD/ITD servers, located on City premises on SPD networks. Access to these networks is as specified in 4.1. All data that goes to mobile clients are encrypted to FIP 140-2 standards and is therefore CJIS compliant.

Per the CJIS Security Policy:

"Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunication lines; personnel security to include background screening requirements; technical security to protect against unauthorized use; data security to include III use, dissemination, and logging; and security of criminal history 08/16/2018 CJISD-ITS-DOC-08140-5.7 D-3 records. Additionally, each CSO must ensure that all agencies establish an information security structure that provides for an ISO and complies with the CJIS Security Policy.

Network Diagrams - Network diagrams, i.e. topological drawings, are an essential part of solid network security. Through graphical illustration, a comprehensive network diagram provides the "big picture" – enabling network managers to quickly ascertain the interconnecting nodes of a network for a multitude of purposes, including troubleshooting and optimization. Network diagrams are integral to demonstrating the manner in which each agency ensures criminal justice data is afforded appropriate technical security protections and is protected during transit and at rest."

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. In addition, the Office of Inspector General can access all data and audit for compliance at any time.

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

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

If improperly collected data is found during an audit log review (or through other means), it will be deleted from the server (includes a soft delete and purging of deleted records). The user responsible for the improper collection will be dealt with on a case-by-case basis, to include limiting their access to data or removal of their access to the system altogether.

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 7.110v 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.

Per the CJIS Security Policy:

"5.8.3 Digital Media Sanitization and Disposal The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

5.8.4 Disposal of Physical Media Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel."

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.

SPD's Intelligence and Analysis Section reviews the audit logs and ensures compliance with all regulations and requirements.

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?

No person, outside of SPD and Seattle IT, has direct access to the application or the data.

As Seattle IT supports the iBase 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 iBase system through inter-departmental partnership. The MCA can be found in the appendices of this SIR.

Because all the data used in this project relates to criminal investigations, any information shared will follow standard policing practices and CJIS compliance.

6.2 Why is data sharing necessary?

Data sharing is frequently necessary during the course of a criminal investigation to follow up on leads and gather information on suspects from outside law enforcement agencies. Cooperation between law enforcement agencies is an essential part of the investigative process. For example, an investigator may send out a photo or description of a homicide suspect in order to find out if another LE agency knows their identity.

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

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

Yes ☒ No ☐

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

All users with direct access to the data must have a Seattle Police Department network account. The software is not set up to allow any other agency to access the data.

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?

No additional data sharing agreements have been established regarding the iBase system or the data it contains.

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

This software simply visualizes the data already available to investigators as part of their criminal investigations. The data collected in this database mirrors that in SPD's RMS/CAD, so no additional accuracy check is required for that data. All manually added information must include the source description, source reliability, and content certainty.

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

As per RCW 10.97, individuals who are subject to a criminal investigation will not be party to the information collection process and thus will not have an opportunity to correct their information. Detectives or other sworn officers may interview such subjects or conduct additional investigation to determine inaccuracies in the information, on a case by case, basis.

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?

IBM Security i2 iBase system is used during the investigation of crimes by the SPD Real Time Crime Center and information collected and stored in the system is related to these criminal investigations.

All use of the i2 iBase system must also comply with SPD Policy 12.050 – Criminal Justice Information Systems and may only be used for legitimate criminal investigative purposes.

Use of the iBase system will be governed by the City of Seattle Intelligence Ordinance, 28 CFR Part 23, CJIS requirements, and any future applicable requirements.

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

Users of the iBase system and i2 Analyst's Notebook undergo training on the use of the software, which includes privacy training.

All authorized users of the iBase system must be CJIS certified and must maintain Washington State ACCESS certification.

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.

The CJIS training requirements can be found in the appendices of this document, as well as in question 3.3, above.

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.

The nature of the Department's mission will inevitably lead it to collect and maintain information many may believe to be private and potentially embarrassing. Minimizing privacy risks revolve around disclosure of personally identifiable information.

The primary privacy risk with this system pertains to Personally Identifiable Information (PII) being added on individuals not directly associated with criminal activity. To mitigate this risk, users only add PII on individuals associated with a criminal investigation and/or collected in accordance with the City of Seattle Intelligence Ordinance. In addition, SPD conducts regular reviews of audit logs to ensure proper use and retention of the data.

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." iBase is not used to track demonstration participants and no demonstration-related images have been input into the iBase system.

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 public may express concern over the consolidation of so much information about individuals, but all of the data that is included in the iBase system is already available to investigators in RMS/CAD and other legally accessible information repositories; this project simply works to make accessing and analyzing that information more efficient. Every individual in the database is related to a criminal investigation or part of an investigation under the City of Seattle Intelligence Ordinance. Under no circumstances will this project involve the collection of Personally Identifiable Information (PII) on people with no connection to criminal investigations or related to a Seattle Police response to an incident.

8.0 Monitoring and Enforcement

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

The information used in iBase system relates to ongoing criminal investigations. Information will be released in response to public disclosure requests as applicable under the Public Records Act and the City of Seattle Intelligence Ordinance, just as they are applicable to any other SPD investigative records.

Per SPD Policy 12.080, 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.

This software is not directly accessed by outside agencies. Information may be shared with outside agencies as it would with any criminal investigation and release is governed by the same rules. Any bulletins or other notifications created with information or analysis resulting from this project are kept in the SPD network file system as well as recorded in the established SPD bulletin system. In addition, the software's audit log keeps a record of all data accessed by each user.

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 software's audit log tracks all log-ins/offs, data views, and data modifications. SPD periodically reviews these logs to ensure proper use of the software. In addition, the logs are available at any time for review by the Seattle Intelligence Ordinance Auditor.

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
06/06/17	01/04/18	$67,860	$113,615	$17,314	Federal Grant

Notes:

SPD has received a Department of Justice grant in order to build out the technology available to the RTCC.

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
$12,325	0	0	$4,713.97	SPD Budget

Notes:

The primary ongoing cost of this project is the annual iBase licenses. Maintenance of the software and servers is handled by SPD and Seattle IT.

1.3 Cost savings potential through use of the technology

Quantifying the cost savings through this technology is difficult as the primary purpose is to improve the department's effectiveness at reducing crime and improving public safety. While no formal study was done of the time previously wasted on manually re-entering information onto a chart, adding a single person's criminal history to a chart could take multiple days of work. With this software, a user can see a subject's criminal history in minutes. The man-hours saved on such tasks saves the department money, while also enhancing the department's overall understanding of crime within the City of Seattle.

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

Additional federal grants could be acquired to pay the continued licensing fees of the software.

Expertise and References

Purpose

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

1.0 Other Government References

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

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

2.0 Academics, Consultants, and Other Experts

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

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

3.0 White Papers or Other Documents

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

Title	Publication	Link
Application of Link Analysis to Police Intelligence	*HUMAN FACTORS* Volume:17 Issue :2 Dated:(APRIL 1975) Pages:157-164	https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=45467
Police Information Systems and Intelligence Systems	United Nations Office on Drugs and Crime	https://www.un.org/ruleoflaw/files/4_Police_Information_Intelligence_Systems.pdf
Investigative Analysis in Law Enforcement	IBM Solution Brief	https://www.ibm.com/downloads/cas/OW3KJN1Y

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?

Some personally identifiable information (PII) gathered during criminal investigations could be used to identify individuals who are associates of criminal suspects, such as their name, home address or contact information. Victims of criminal activity may also be identified during incident responses, whose identities should be protected in accordance with RCW 42.56.240 and RCW 70.02. SPD mitigates these risks by entering information into the iBase system only when it is related to the investigation of a crime and/or collected in accordance with the City of Seattle Intelligence Ordinance. In addition, SPD conducts regular reviews of audit logs to ensure proper use and retention of the data.

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

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

The mission of the Seattle Police Department is to prevent crime, enforce the law, and support quality public safety by delivering respectful, professional, and dependable police services. To mitigate against any potential algorithmic bias or ethnic bias to emerge in the use of link analysis software such as the iBase system, SPD employees are responsible for gathering, creating, and disseminating information (internally or externally as defined above) and are bound by SPD Policy 5.140 which forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

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?

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

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

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

IBM Security i2 iBase system is used during the investigation of crimes by the SPD Real Time Crime Center and information collected and stored in the system is related to these criminal investigations. There is no distinction in the levels of service this system provides to the various and diverse neighborhoods, communities, or individuals within the city.

All use of the i2 iBase system must also comply with SPD Policy 12.050 – Criminal Justice Information Systems and may only be used for legitimate criminal investigative purposes.

Use of the iBase system is be governed by the City of Seattle Intelligence Ordinance, 28 CFR Part 23, CJIS requirements, and any future applicable requirements.

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

In an effort to mitigate the possibility of disparate impact on historically targeted communities, SPD has established policies regarding the dissemination of data in connection with criminal prosecutions, Washington Public Records Act (Chapter 42.56 RCW), and other authorized researchers.

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

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

Like decisions around data sharing, data storage and retention have similar potential for disparate impact on historically targeted communities. The information stored within the iBase system is related only to criminal investigations and its users are subject to SPD's existing policies prohibiting bias-based policing. Further, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

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

The most important unintended possible consequence related to the continued utilization of the iBase system is the possibility that erroneous links between individuals related to criminal investigations may be considered. However, because all analysis conducted in the RTCC is developed manually by analysts the risk is mitigated by the efficiencies provided by the use of the iBase system.

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.	2.	3.

2.1 Scheduled public meeting(s).

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

Location	
Time	
Capacity	
Link to URL Invite	

2.2 Scheduled focus Group Meeting(s)

Meeting 1

Community Engaged	
Date	

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 Response

Description

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

Purpose

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

Benefits to the Public

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

Privacy and Civil Liberties Considerations

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

Summary

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

Appendix A: Glossary

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

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

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

DON: "department of neighborhoods."

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

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

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

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

OCR: "Office of Civil Rights."

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

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

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

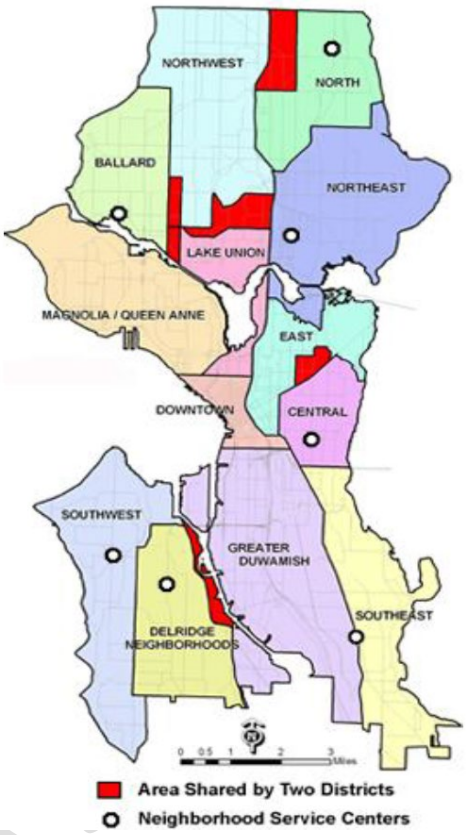
RET: "racial equity toolkit"

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

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

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

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



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

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