SEATTLE CITY COUNCIL
CENTRAL STAFF

April 19, 2022

MEMORANDUM

To: Economic Development, Technology and City Light Committee
From: Lise Kaye, Analyst
Subject: Council Bill 120309 - Authorizing approval of uses and accepting the surveillance impact report for the Seattle Police Department's use of IBM's i2 iBase Link Analysis Software

On Wednesday, April 27, 2022, the Economic Development, Technology and City Light Committee will discuss Council Bill 120309. This Council Bill would approve the Seattle Police Department's (SPD's) continued use of IBM's i2 iBase Link Analysis Software and accept the Surveillance Impact Report (SIR) and an Executive Overview for this technology. The bill is intended to meet the requirements of Seattle Municipal Code Chapter 14.18, Acquisition and Use of Surveillance Technologies, which requires City of Seattle departments intending to acquire surveillance technology to obtain advance Council approval of that acquisition and of a surveillance impact report (SIR).[1] Departments must also submit a SIR for surveillance technology in use when Ordinance 125376 was adopted in 2017 (referred to in the ordinance as "retroactive technologies"), but failure to approve an ordinance for a retroactive technology does not require SPD to discontinue its use. Councilmembers may choose to amend the ordinance to request additional information or to request that SPD develop new and/or revised operational policies, which, if implemented, could restrict or modify the application of certain technologies.

This memo describes IBM's i2 iBase Link Analysis Software, summarizes recommendations from the Community Surveillance Working Group, describes whether and how each recommendation is addressed in the SIR and/or by current law, and summarizes responses by the Chief Technology Officer (CTO) and/or SPD. Finally, the memo identifies policy issues for Council consideration.

IBM's i2 iBase Link Analysis Software

IBM's i2 iBase Link Analysis Software (iBase) is a relational database that SPD uses to combine and analyze different types of data associated with police investigations. Specifically, SPD's "Real Time Crime Center" (RTCC) uses this software to combine data from its Records Management System (RMS) and the Computer Aided Dispatch (CAD) system with information gathered during criminal investigations and then to portray that information visually on a chart or other display[2]. The visual displays help analysts and investigators see connections between known entities, vehicles, locations, and other data. SPD uses these analyses to assist ongoing criminal investigations and to provide information to officers in the field. The SIR identifies the risk of erroneous links between individuals not related to criminal investigations as the most important unintended civil liberties consequence from this technology. According to SPD, that risk is mitigated because iBase makes it

[1] The Executive Overview summarizes SPD's allowable uses of IBM i2 iBase. See also the memo summarizing process for developing a Surveillance Impact Report (SIR), consistent with Ordinances 125376 and 125679 and Ordinance 108333, Seattle's "Intelligence Ordinance," adopted in 1979 and amended in 1982 via adoption of Ordinance 100572.

[2] Displays include heatmaps (per Wikipedia, a data visualization technique that shows magnitude of a phenomenon as color in two dimensions), relationships and diagrams.

easier for users to identify erroneous linkages in existing data. SPD mitigates other risks, such as acquisition of private data about individuals, potential algorithmic bias or ethnic bias, and potential racial or ethnicity-based bias in data sharing, storage and retention by only entering information into iBase related to the investigation of a crime and/or collected in accordance with the City's Intelligence Ordinance (SMC 14.12). SPD provides additional mitigation through its evidence procedures, anti-bias policies and warrant parameters. The RET does not identify metrics to be used as part of the CTO's required annual equity assessments.

Surveillance Working Group Recommendations and CTO Response

The Community Surveillance Working Group's Impact Assessment for iBase makes 15 recommendations to Council. The CTO's response finds that the "policy, training and technology limitations enacted by SPD provide adequate mitigation for the potential privacy and civil liberties concerns raised by the Working Group." The CTO's response does not specifically address the Working Group's recommendations, but it identifies relevant citations from the SIR for each of the "key concerns" raised by the Working Group. **Table 1** describes whether the SIR as drafted or current law addresses the Working Group's recommendations, as well as relevant responses from the CTO and/or SPD.

Table 1. Working Group Recommendations

Working Group Recommendation	Whether/How Addressed by SIR, CTO or SPD and/or Current Law
1. The purpose and allowable uses of i2 iBase must be clearly defined, and any SPD use of i2 iBase must be limited to that specific purpose and those allowable uses. The specific incident types for which i2 iBase may be used must be clearly stated. The use limits must restrict when someone's relationship network may be assembled in i2 iBase.	**Executive Overview.** Operational Policies represent the only allowable uses of the equipment and data collected by this technology. **SIR §3.2 …** 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. **SIR §4.3** … iBase is used to assist with criminal investigations and to provide actionable information to units in the field. *SMC 14.12 (the "Intelligence Ordinance) governs the collection of data for a criminal investigation.* *The SIR does not limit the use of iBase to specific incident types or define when an individual's network may assembled.*
2. If SPD's use of i2 iBase is governed by a contract, it must be made publicly available.	Not addressed in the SIR. *Seattle's Information and Technology Department (ITD) has a contract with IBM for its two annual licenses.*
3. SPD must publicly disclose all of its data sources, such as data brokers (e.g., LexisNexis, CoreLogic) and any use of non-public details from social media platforms (e.g., Facebook, Twitter).	**SIR §4.1** … information pulled into iBase automatically comes from SPD's Records Management System (RMS), Computer Aided Dispatch (CAD) system, and information … collected during the course of a criminal investigation…. *According to SPD, the department does not enter data from any data brokers into iBase. Open source information obtained during the course of a criminal investigation may be entered into iBase. No social media data that is not open source/publicly available is entered into iBase, even if it was obtained during the course of a criminal investigation.*

Working Group Recommendation	Whether/How Addressed by SIR, CTO or SPD and/or Current Law
4. SPD must not be permitted to share i2 iBase data with third parties	**SIR §6.1** No person, outside of SPD and Seattle IT, has direct access to the application or the data.... Because all the data used in this project relates to criminal investigations, any information shared will follow standard policing practices and CJIS compliance.
5. There must be a regular audit to assess for biases in the data imported into i2 iBase and in the analyses generated by i2 iBase. There must be technical mechanisms in place to enable robust auditing to occur (e.g., detailed logs).	**SIR §8.2** SPD's Audit, Policy and Research Section is authorized to conduct audits of all investigative data collection software and systems, and the Office of Inspector General for Public Safety and the federal monitor can conduct audits of the software and its use at any time. *According to SPD, the audit log tracks every action a user takes (e.g., searching, accessing data, adding data, editing data).*
6. There must be limits on the kinds of data that may be inputted both manually and automatically into i2 iBase, ensuring that additional pools of public or private information are not added in the future.	Not addressed in the SIR. *According to SPD, iBase users may manually add data to iBase that has already been obtained during the course of a criminal investigation. Information collection is governed by SMC 14.12 (the "Intelligence Ordinance) and federal regulations (28 CFR Part 23 and Criminal Justice Information System requirements).*
7. There must be a shortened data retention period that does not exceed the time necessary to conduct a criminal investigation.	**SIR §4.0** All manually added information is deleted from the system after five years. *The State Law Enforcement Records Retention Schedule for Intelligence Files requires retention "until no longer needed for agency business." However, federal law allows for a retention period of up to five years, so SPD applies that period to all manually entered data.*[3]
8. There must be a clear deletion oversight process to ensure that manually added data are deleted after the specified retention period.	**SIR §1.2** SPD conducts regular reviews of audit logs to ensure proper use and retention of data. *According to SPD, iBase has an automated query that alerts users that manually entered data is approaching its 5-year limit (at 4 years, 9 months and again at 4 years, 11 months), at which point users purge the data from the system through the "batch delete" feature.*
9. There must be a requirement that limits employee access to i2 iBase records.	Not addressed in the SIR. *According to SPD, two civilian SPD analysts and one civilian Seattle IT employee currently have access to iBase. Only the two civilian analysts are currently able to produce such visualizations for detectives, but multiple detectives might request such assistance.*

[3] Section 8.2 of the State Law Enforcement Records Retention Schedule establishes different retention periods for different types of Intelligence records. 28 CFR Part 23.20(h) establishes a retention period not to exceed five years.

Working Group Recommendation	Whether/How Addressed by SIR, CTO or SPD and/or Current Law
10. There must be a manual relationships analysis process that includes clear checkpoints designed to ensure erroneous data and inaccurate linkages generated by i2 iBase are detected and corrected before they are actively investigated.	**SIR §4.2** … when manually adding information, a user must provide the source description, source reliability, and content certainty… **SIR §5.3** provides for deletion of improperly collected data found during an audit log review
11. There must be limits on usage of potentially erroneous i2 iBase analyses and search data in rapid-response settings where manual analysis is not possible.	Not addressed in the SIR. *SPD's use of data from an iBase analysis is an operations issue is governed by the SMC 14.12 (the "Intelligence Ordinance), which governs SPD's collection of data for a criminal investigation.* *According to SPD, the department primarily uses iBase for long-term criminal investigations; during time-sensitive investigations, iBase data may be searched, along with searches of RMS, CAD, and relevant files.*
12. There must be a requirement for SPD to disclose for how many incidents per year they use i2 iBase.	Not addressed in the SIR. *According to SPD, it would not be possible to track this information, as a single search may result in dozens or more incidents laid out on a chart for analysis.*
13. There must be a requirement that the use of i2 iBase is always disclosed to the individual or the legal representative of an individual facing charges for which i2 iBase was used in an SPD investigation.	**SIR §6.6** As per RCW 10.97, individuals who are subject to a criminal investigation will not be party to the information collection process…[4]
14. There must be a regulation prohibiting the use of i2 iBase for predictive policing.	Not addressed in the SIR. *According to SPD, data compiled via iBase is never used for predictive purposes. It is a tool to assist in investigation of crimes that have already occurred.*
15. There must be a contract with IBM that ensures IBM never possesses, uses, or accesses SPD data.	Not addressed in the SIR. *According to SPD, Seattle's Information and Technology Department (ITD) has a contract with IBM for its two annual licenses and IBM does not have access to SPD's iBase data.*

[4] RCW 10.97.080 – "… The individual's right to access and review of criminal history record information shall not extend to data contained in intelligence, investigative, or other related files….

Policy Considerations

Central Staff has identified the following potential policy considerations and options.

1. Annual equity assessment metrics. SPD has not yet finalized metrics to be used in evaluating use of i2 iBase as part of the CTO's annual equity assessments. These assessments are intended to play a key role in determining whether the City's surveillance legislation is meeting the goals of the Race and Social Justice Initiative. In the absence of such metrics, it is unclear how SPD and/or the CTO could identify disproportionate impacts from the use of i2 iBase, such as the frequency of specific populations appearing on i2 iBase displays.

   Options:

   A. Council may wish to request a report on the proposed metrics by a date certain.

   B. Take no action.

2. Response to Public Comments. The SIR does not provide a response to question 4.1 "How will you address the concerns that have been identified by the public."

   Options:

   A. Request that SPD provide a written response to public comments associated with the SIR public engagement process by a date certain.

   B. Take no action.

3. Mitigation of civil liberties impacts. The SIR flags the risk of erroneous links between individuals not related to criminal investigations as the most important unintended consequence from the use of this technology. The SIR also identifies data sharing, storage and retention as having the potential to contribute to structural racism and/or disparate impacts on historically targeted communities. An expanded evaluation of these risks and related concerns could reveal whether more direct policies and protocols would better protect against errors, potential bias in baseline data, and/or disproportionate over-surveillance.

   Options:

   A. Obtain an independent evaluation of the civil liberties risks associated with the use of iBase, including potential bias in its baseline data sources, the data manually input into iBase, data validation and accuracy of analyses, and demographic information about the individuals and groups associated with each iBase visualization.

   B. Take no action.

4. Contractual Terms – Data and Security Protection. SPD reports that ITD has a contract with IBM for annual licenses for i2 iBase, which only covers the annual subscription cost. The lack of a contract and/or reliance upon a vendor-provided licensing agreement may reduce the City's ability to restrict IBM's access to sensitive and/or private information.[5]

   Options:

   A. Request that SPD contractually ensures data and security protection of personally identifiable information or sensitive information generated or otherwise obtained through the use of iBase. This may require additional resources, potentially through a supplemental budget action.

   B. Take no action.

5. Retention schedule. The i2 iBase system automatically deletes manually entered data after five years. SPD uses the maximum, rather than the minimum, retention periods allowed by state and federal law. As noted above (see footnote 3), federal policies establish a retention period not to exceed five years. Extended records retention could result in maintaining inaccurate and/or out of date information.

   Options:

   A. Request that SPD develop a policy for retention of iBase records that complies with the minimum retention period allowed by state and federal law and that requires regular review and validation of iBase records retained for more than one year.

   B. Take no action.

6. Data sharing with Community Safety and Communications Center. The SIR describes how the iBase system uses data from SPD's Computer Aided Dispatch (CAD) system, however, new data sharing protocols should be developed since the CAD system is now housed within the Community Safety and Communications Center.

   Options:

   A. Request that SPD develop a formal agreement with the CSCC establishing common protocols for data retention and sharing of data.

   B. Take no action.

cc: Aly Pennucci, Deputy Director
Brian Goodnight, Supervising Analyst

[5] Data and security protection for the City's data may not be included by vendors in their standard licensing agreements for off-the-shelf products or for "software as a service" products, in which an application is accessed via a cloud provider. ITD incorporates data and security protection requirements into its purchasing contracts, and Finance and Administration Department's contract template for purchasing technology has similar terms.