



Seattle Office of Inspector General

Surveillance Technology Usage Review i2 iBase Link Analysis Software (2022)

As Required by Seattle Municipal Code 14.18.060

September 29, 2023

Office of Inspector General
City of Seattle
PO Box 94764
Seattle, WA 98124-7064
oig@seattle.gov
(206) 684-3663



Purpose

Surveillance Ordinance Requirements

Per Seattle Municipal Code 14.18.060, OIG is required to annually review the Seattle Police Department (SPD) use of surveillance technology to assess compliance with the requirements of Chapter 14.18.

Non-Audit Statement

This review was not conducted under Generally Accepted Government Auditing Standards (GAGAS); however, OIG has followed GAGAS standards regarding the sufficiency and appropriateness of evidence.





Table of Contents

Executive Summary	2
Technology Description	4
A. 2022 Surveillance Technology Usage.....	5
B. Data Sharing with External Partners and Other Entities	7
C. Data Management and Safeguarding of Individual Information.....	8
D. Impact on Civil Liberties and Disproportionate Effects on Disadvantaged Populations.	10
E. Complaints, Concerns and Other Assessments.....	11
F. Total Annual Costs.....	12





Executive Summary

The summary below highlights significant audit findings and recommendations regarding compliance with SMC 14.18.060.

14.18.060 Provision	Compliance Determination	Auditor's Findings	Recommendations
A. How surveillance technology has been used, usage frequency, and whether usage patterns have changed.	Yes 	i2 iBase visualization charts were created for homicide, robbery, kidnapping, and shooting investigations in 2022. No information other than law enforcement data were used within the charts.	No recommendations.
B. How often surveillance technology or its data is shared with other entities, including government agencies.	Yes 	In 2022, one i2 iBase chart was shared with the King County Prosecuting Attorney's Office. Charts may also have been shown to other law enforcement agencies during regional meetings, but no copies were given to these agencies.	No recommendations.
C. How well data management protocols are safeguarding individual (personal) information.	Yes 	In general, i2 iBase and the i2 Analyst's Notebook follow best practices for data management and security.	No recommendations.
D. How deployment of surveillance technologies impacted or could impact civil liberties or have disproportionate effects on disadvantaged populations, and how those impacts are being mitigated.	Yes 	OIG reviewed all analysis charts for the review period. In no instance did OIG observe data sourced from social media, or the technology being used for predictive policing.	No recommendations.



14.18.060 Provision	Compliance Determination	Auditor's Findings	Recommendations
E. A summary of any complaints or concerns about the surveillance technology and results of internal audits or assessments of code compliance.	Yes 	No complaints or concerns were submitted to the City in 2022.	No recommendations.
F. Total annual costs for use of surveillance technology, including personnel and other ongoing costs.	Yes 	Total 2022 costs were in the amount of \$24,491.80.	No recommendations.



Technology Description

*The **Real Time Crime Center** is the information “hub” of SPD where resources and collective knowledge are utilized to enhance SPD’s effectiveness at reducing crime and improving public safety.*

*SPD’s **Records Management System (RMS)** is Mark43.*

***Computer-Aided Dispatch (CAD)** is a software utilized by SPD’s 9-1-1 Center that enables real-time documentation of SPD’s response to calls for service, including relevant information obtained by responding officers.*

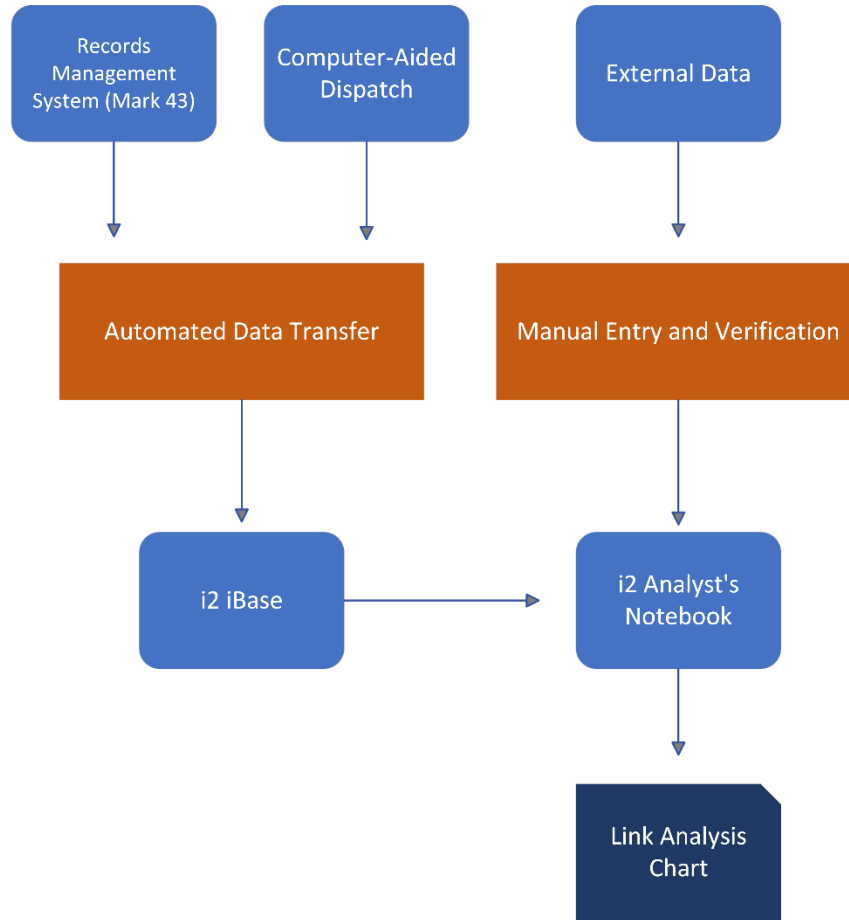
i2 iBase is the back-end server software for the i2 Analyst’s Notebook application, a software system that organizes existing SPD data into visually accessible information. When paired with the i2 Analyst’s Notebook, this link analysis software works as a relational database application and a visual analysis tool used by analysts within the Seattle Police Department’s (SPD) **Real Time Crime Center (RTCC)**. The software consists of a wide range of analytical tools used by the RTCC to map and transform data from SPD’s **Records Management System (RMS)**, **Computer-Aided Dispatch (CAD)**, and other legally accessible information repositories. The purpose of this technology is to capture, analyze, and display existing SPD data to assist analysts with better understanding criminal conspiracy networks, the chronology of events in a case, and the associations between victims, suspects, and locations.

There are two i2 iBase Link Analysis Software applications used by SPD: i2 iBase and the i2 Analyst’s Notebook. i2 iBase is an on-premise, security-encrypted SQL server that serves as the data repository for the system. Data from RMS and CAD are transferred into the i2 iBase repository via a one-way, automated electronic data transfer. The i2 Analyst’s Notebook serves as the interface to i2 iBase and is a locally installed software found on the workstations of RTCC analysts. Data from the repository are added directly onto an i2 Analyst’s Notebook chart (i.e., a digital “link board” or “pin board”), along with data manually entered by RTCC staff. These charts are then used by SPD investigations personnel for operational crime analysis.

The i2 iBase Link Analysis Software is used solely by trained and CJIS-certified RTCC analysts and supporting Seattle IT employees. Though SPD investigations personnel are the consumers of the i2 iBase visualization charts, they do not have direct access to either component of the technology. Only RTCC analysts are authorized to use this technology to support SPD investigations, as they are responsible for gathering information from RMS and CAD, manually adding law enforcement data into the i2 iBase system and generating link analysis charts.



i2 iBase Data Flow



A. 2022 Surveillance Technology Usage

SMC 14.18.060, § A:
How surveillance technology has been used, how frequently, and whether usage patterns are changing over time.

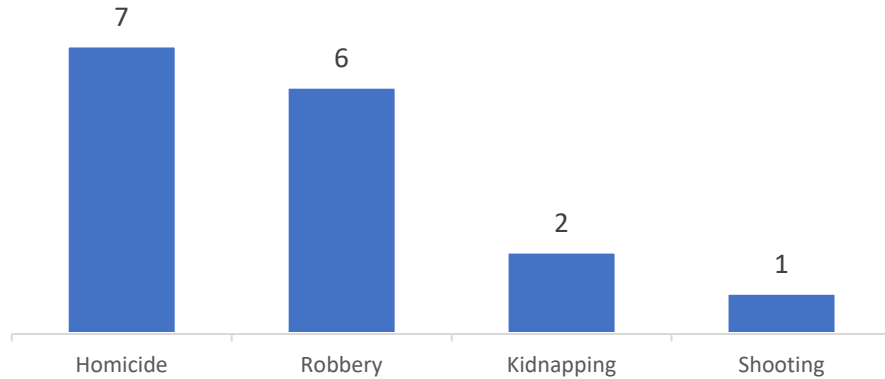
The RTCC created eleven i2 iBase visualization charts for thirty-one unique cases during the 2022 review period. Each chart was modeled and visualized using data imported from RMS and/or external data gathered by SPD investigators. OIG reviewed all visualization charts produced by RTCC staff in 2022 for types of criminal activity investigated, data sources, and compliance with the SIR for this technology.

In 2022, there were four types of criminal activity charted with i2 iBase; homicide, robbery, kidnapping, and shootings.



Types of Criminal Activity Analyzed in 2022

Among 11 Visualization Charts



Entities are subjects, vehicles, and addresses.

Links are the relationships and connections between entities.

National Integrated Ballistic Information Network (NIBIN) is a national database and investigative tool used by law enforcement agencies to determine whether ballistic evidence has been used in previous crimes.

The visualizations created for these investigations were link analysis charts (i.e., digital “link boards” or “pin boards”) consisting of **entities**, **links**, and other attributes pertaining to each case. Each chart was designed to provide a graphic representation of each incident along with visualizations of case entities and their associations. Firearms and other weaponry associated with specific incidents were visualized for gun tracing and included information such as gun registries and ballistic information obtained from the **National Integrated Ballistic Information Network (NIBIN)**.

OIG reviewed the link analysis charts and found the total number of entities varied depending on the circumstances of each case and ranged from as few as ten data nodes to approximately three-hundred. In all cases, data from RMS (i.e., names, dates of birth, location information, and criminal histories) represented most of the information, and OIG observed limited manual entries of external data.

External data included information from other law enforcement agencies, NIBIN hits, and additional information collected during the course of investigations. When manually entering this data, RTCC analysts also complete three different forms to confirm the reliability and credibility of the added information.

According to RTCC personnel, no information other than law enforcement data (i.e., data from RMS, NIBIN, SPD investigators, and other law enforcement repositories) were used within the 2022



link analysis charts. CAD information, while a source system for this technology, was rarely included as SPD considers its data to be less reliable compared to the verified information found within RMS.

Once the link analysis charts are constructed, charts are given to SPD investigations personnel in PDF format for review and analysis. SPD detectives utilize the charts to better understand their criminal investigations such as the events and patterns within criminal activities, the structure and operations of criminal networks, and the identities and relationships between key individuals.

B. Data Sharing with External Partners and Other Entities

SMC 14.18.060, § B:
*How often
surveillance
technology or its
data are being
shared with other
entities, including
other governments
in particular.*

Data sharing between law enforcement agencies occurs frequently during SPD investigations and is considered an essential part of the investigative process. Information sharing between these agencies allows investigators to pursue leads and gather additional information on key suspects and events. Since most of the information contained within i2 iBase charts stems from criminal investigations, any information shared from the i2 iBase technology is classified as law enforcement sensitive and must be in compliance with CJIS and standard policing practices.

According to the RTCC, analysts share i2 iBase charts directly with outside law enforcement agencies when requested. When sharing these records, charts are converted to PDF format (to preserve the integrity of the data) and shared via CJIS-compliant, security-encrypted emails once permission has been granted by the investigation's lead detective. Charts may also be shared with other entities, along with other materials associated with a case, to aid them in chronologizing events or showing established associations between suspects, victims, weapons, vehicles, and locations. Per RTCC personnel, a physical copy of one conspiracy chart was shared with the King County Prosecuting Attorney's Office in 2022. Charts may have also been shown to other law enforcement agencies during regional meetings, but no copies were given to these agencies.

i2 iBase charts may also be shared in response to public disclosure requests pursuant to the Washington Public Records Act, Chapter

42.56 RCW. These requests are managed by SPD's Legal Unit and tracked through SPD's Public Records Request Center. According to SPD, no records related to the i2 iBase technology were shared via public disclosure requests or SPD's Records Unit in 2022.

C. Data Management and Safeguarding of Individual Information

SMC 14.18.060, § C:

How well data management protocols are safeguarding individual information.

Data Types

i2 iBase and the i2 Analyst's Notebook application allow SPD analysts to build a map of the relationships between suspects, vehicles, weapons and other physical items and the criminal incidents in which their involvement is suspected. As a result, the data set in i2 iBase contains personal identifiable information (PII) for suspects and potentially for victims of crime. The data set also includes information about the relationships of suspects with others, such as familial ties, employment, or gang affiliation. Suspect relationship analysis based on political or religious affiliation is generally prohibited by both municipal code and SPD policy, and our review found no evidence that i2 iBase and i2 Analyst's Notebook are used to perform such analysis.

Data Sources

When an analyst begins work on a new case, they input the General Offense (GO) number associated with that case, and the i2 iBase system automatically imports available information about people, locations, vehicles, weapons, and property relevant to that particular case from CAD and Mark43. Analysts can also manually add new relationships once this import process is complete.

i2 Analyst's Notebook has the capability to graph social data captured from warrant returns on suspect mobile phones, however SPD personnel indicated that such information would not be useful, as it would clutter their analysis and make it difficult to discern meaningful patterns.

SPD personnel also stated that they do not purchase commercially available data to be manually or automatically added to this system. Nor, at present, is suspect relationship data added into the i2 Analyst's Notebook from the Washington State Intelligence Fusion Center, FBI, or other external law enforcement sources.

Data Retention

Information imported from the Mark43 RMS or CAD systems is retained indefinitely. Information added manually by analysts is retained for 5 years, then purged. The most recent 5 years of manually added information is purged via a manual query and delete process that is performed once per month. Once complete, the individual responsible for purging the data checks a box in the i2 iBase application, which notes that the purge was completed in the system's audit log.

Vendor Privacy and Security

The i2 Group, a wholly owned subsidiary of L3 Harris, is the current vendor of the i2 iBase and i2 Analyst's Notebook software, as L3 Harris acquired the i2 portfolio from IBM in 2022. L3 Harris has achieved the AICPA SOC2 and ISO 27001 security compliance certifications, which indicate their security and data management policies, practices, and capabilities have been approved by an independent auditor.

The License Agreement¹ and Data Processing Addendum² are posted on the i2 Group's website and were included in this review. Section 2.3 of the i2 Data Processing Addendum (USA Only) states:

"2.3 Restrictions. Except as otherwise permitted by Data Protection Laws, i2 shall not (a) sell or share (as such terms are defined by Data Protection Laws) Client Personal Data; (b) retain, use, or disclose the Client Personal Data for any purpose other than for the business purposes specified in the Agreement; (c) retain, use, or disclose Client Personal Data outside of the direct business relationship between i2 and Client; and (d) combine the Client Personal Data with personal information that i2 receives from or on behalf of another person or persons, or collects from its own interaction with the applicable Data Subject. i2 understands the restrictions set forth herein and will comply with them."

¹ <https://734313.fs1.hubspotusercontent-na1.net/hubfs/734313/legal/i2-license-agreement.pdf>

² <https://734313.fs1.hubspotusercontent-na1.net/hubfs/734313/Data-Processing-Addendum-USA-Only.pdf>



Authentication and Authorization

The i2 iBase and i2 Analyst’s Notebook software can only be accessed by an SPD-managed computer on the SPD internal network. Analysts must log in using their Azure Active Directory Single Sign-On credentials, then complete an MFA challenge by swiping a physical token at a reader when logging into their computer.

Backups

The i2 iBase software configuration and Windows server state is backed up nightly, however the database containing relationship data is excluded from the backup process, which mitigates the risk of accidentally retaining data improperly via the backup process.

D. Impact on Civil Liberties and Disproportionate Effects on Disadvantaged Populations

SMC 14.18.060, § D:
How deployment of surveillance technologies impacted or could impact civil liberties or have disproportionate effects on disadvantaged populations [...].

Two relevant concerns were raised in the Privacy and Civil Liberties Assessment section of the Surveillance Impact Report (SIR) pertaining to impacts on civil liberties. These concerns were:

- The absence of usage limits for i2 iBase and the potential for predictive policing; and
- The incorporation of social media information into the i2 iBase software.

Absence of Usage Limits and Potential for Predictive Policing

Community members expressed concern that the absence of usage limits in SPD policy had the potential to allow SPD to use the vast amounts of data within i2 iBase for **predictive policing**. To address these concerns, OIG interviewed the RTCC analysts who managed this system, and reviewed all analysis charts created by RTCC personnel for the review period. In no instance did we observe the technology being used for predictive policing. Further, as a software currently configured to only visualize existing records, it appears unlikely to be suitable for such use at this time. OIG will continue to monitor these community concerns in future reviews.

Predictive policing
is the process of using mathematics and computer algorithms to analyze substantial amounts of data for the purpose of anticipating future criminal activity.

Social Media

Another community concern was the potential for non-public social media information to be used as an i2 iBase data source. The concern was that SPD officers may use alias accounts to obtain non-public information from social media platforms for importation and analysis within the i2 iBase software.

RTCC personnel identified that plugins are available for the i2 Analyst's Notebook which would allow analysts to incorporate data from social media into their link analysis process. However, OIG observed that the relevant plugins were not installed, and per RTCC personnel, working with the vendor to enable the social media plugins would come at significant cost and IT configuration difficulties for the Department. Personnel expressed that they see no need to purchase the plugin, nor do they manually collect or include social media data in their analyses. OIG did not observe data sourced from social media within link analysis charts from 2022. OIG will continue to monitor this issue in future reviews.

E. Complaints, Concerns and Other Assessments

SMC 14.18.060, § E:
A summary of any complaints or concerns received by or known by departments about their surveillance technology and results of any internal audits or other assessments of code compliance.

Complaints submitted to the Office of Police Accountability (OPA) and the City of Seattle's Customer Service Bureau were reviewed to determine whether any i2 iBase-related concerns were submitted to the City in 2022. RTCC personnel were also interviewed to assess whether any internal audits or assessments of code compliance were conducted during the review period. Below are summaries of the findings.

OPA Complaints

There were no complaints or concerns submitted to OPA regarding the i2 iBase surveillance technology in 2022.

City of Seattle Customer Service Bureau Complaints

There were no complaints submitted to the Customer Service Bureau in 2022 pertaining to SPD's use of the i2 iBase surveillance technology.

Internal Audits or Assessments

OIG is unaware of any audits or assessments conducted by SPD on the i2 iBase technology in 2022.

F. Total Annual Costs

SMC 14.18.060, § F: Annual subscription licenses were identified as the primary ongoing cost for the i2 iBase Link Analysis Software. In 2022, SPD spent a total of \$24,491.80³, which was a combination of the annual subscription and support costs for both iBase (\$11,049.43) and the i2 Analyst's Notebook (\$13,442.37).

Total annual costs for use of surveillance technology, including personnel and other ongoing costs.

No other costs or purchases associated with this technology were identified for that year.

³ This cost total is a prorated figure consisting of combined costs from SPD's 2021 annual contract with IBM (from January 2022 through June 2022) and costs from SPD's 2022 annual contract with i2 Group (from July 2022 through December 2022).