City of Seattle

2021 Surveillance Impact Report Executive Overview

IBM i2 iBase

Seattle Police Department

Overview

The Operational Policy statements in this document represent the only allowable uses of the equipment and data collected by this technology.

This Executive Overview documents information about the collection, use, sharing, security and access controls for data that is gathered through SPD's I2 iBase. All information provided here is contained in the body of the full Surveillance Impact Review (SIR) document but is provided in a condensed format for easier access and consideration.

1.0 Technology Description

The iBase software is a SQL server that imports a portion of the data from SPD's Records Management System (RMS) and Computer Aided Dispatch (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 Real Time Crime Center (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.

2.0 Purpose

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.

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.

3.0 Data Collection and Use

Operational Policy: 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.

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.

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.

4.0 Data Minimization & Retention

Operational Policy: All manually added information is deleted after five years, in accordance with 28 CFR Part 23.

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.

No data outside SPD's RMS/CAD (e.g. commercial data aggregators, publicly available data, or other city departments) is automatically collected.

The software automatically alerts users of data that must be deleted under legal deletion requirements such as 28 CFR Part 23.

5.0 Access & Security

Operational Policy: All SPD employees are backgrounded and access is controlled by SPD Manual Title 12 provisions:

- **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.**

Access

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.”.

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.”

Security

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 data that goes to mobile clients are encrypted to FIP 140-2 standards and is therefore CJIS compliant.

6.0 Data Sharing and Accuracy

Operational Policy: 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.

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.

7.0 Equity Concerns

Operational Policy: 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 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.

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.