POWERFUL TECHNOLOGY SOLUTIONS
FOR THE CITY AND PUBLIC WE SERVE

City of Seattle Privacy Impact Assessment

REAL TIME CRIME CENTER (RTCC) PROJECT

Owner: Seattle Police Department

Date: 12/6/2017

12.7.2017

Seattle
Information Technology

CONTENTS

PURPOSE OF PIA

A Privacy Impact Assessment is designed to outline the anticipated privacy impacts from a City project/program or project/program update that collects, manages, retains or shares personal information from the public. The PIA will provide project/program details that will be used to determine how privacy impacts may be mitigated or reduced in accordance with the City of Seattle Privacy Principles and Privacy Statement.

ABSTRACT

Please provide a brief abstract. *The abstract is the single paragraph that will be used to describe the project and* ***will be published on the Privacy Program website.*** *It should be a minimum of three sentences and a maximum of four, and use the following format:*

- *The first sentence should include the name of the project, technology, pilot, or project/program (hereinafter referred to as "project/program").*
- *The second sentence should be a brief description of the project/program and its function.*
- *The third sentence should explain the reason the project/program is being created or updated and why the PIA is required. This sentence should include the reasons that caused the project/program to be identified as a "privacy sensitive system" in the Privacy Intake Form, such as the project/program requiring personal information, or the technology being considered privacy sensitive.*

This project, the "Real Time Crime Center" (RTCC) project, will increase the efficiency of Seattle Police Department's Real Time Crime Center, which provides actionable information to units in the field to increase officer safety, efficacy, and response to incidents to improve overall public safety. The RTCC will make Computer Aided Dispatch/Records Management System (CAD/RMS) data more readily available to RTCC staff/systems, thus improving RTCC staff ability to monitor and respond to ongoing critical incidents. The current tool set available to the RTCC is often redundant, complex, outdated, and inefficient, preventing RTCC staff from meeting all the desired outcomes of the RTCC project, so better technology is required. The data used by the RTCC relates directly to ongoing cases and therefore will necessarily include personal information about subjects associated with those investigations.

PROJECT/PROGRAM OVERVIEW

Please provide an overview of the project/program. *The overview provides the context and background necessary to understand the project/program's purpose and mission and the justification for operating a privacy sensitive project/program. Include the following:*

- *Describe the purpose of the system, technology, pilot or project/program; the name of the department that owns or is funding the project/program and how it the project/program relates to the department's mission;*
- *Describe how the project/program collects and uses personal information, including a typical transaction that details the life cycle from collection to disposal of the information;*
- *Describe any routine information sharing conducted by the project/program both within City of Seattle departments and with external partners. Describe how such external sharing is designed with the original collection of the information.*

- *Identify any major potential privacy risks identified and briefly discuss overall privacy impact of the project/program on individuals*
- *Identify the technology used and provide a brief description of how it collects information for the project/program.*

The Seattle Police Department (SPD) is currently operating a Real Time Crime Center (RTCC), located at SPD Headquarters. 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 RTCC combines staff, technology, and investigation skills to achieve these goals. SPD has received a Department of Justice grant for $411,539.00 in order to build out the technology available to the RTCC. This build-out is referred to as the Real Time Crime Center Project (RTCC).

The RTCC has been active since late 2015 and has proven successful in augmenting patrol response to incidents by providing information specific to ongoing calls for service. While skilled investigators are the most important part of the RTCC process, better technology is essential for them to operate. Improving access to SPD's data is the single most important step that the department can take to improving the effectiveness of the RTCC. The current tool set is often redundant, complex, and inefficient, preventing RTCC staff from meeting all the desired outcomes of the RTCC.

To that end, the goals of the RTCC are to increase efficiency of investigations, availability of data, awareness of situational information, and timeliness of actionable information to officers on the street. The RTCC project will address these needs by making the data that RTCC staff already uses more readily available to RTCC staff/systems.

Example of Basic RTCC Basic Workflow

- RTCC staff identifies "critical incidents" (initially primarily related to violent crime) as they occur in the city.
- RTCC staff researches information across a variety of systems to gather relevant information to augment the case. This information is researched, analyzed, and shared with units in the field, then recorded in staff logs.
- Staff logs, bulletins, and information from outside agencies are vetted, then saved to a central location accessible by all RTCC staff.
- RTCC staff will draw on this information in future critical incidents, thus improving their response in the future.
- This information is kept in accordance with City of Seattle Intelligence Ordinances, Criminal Justice Information Services (CJIS) regulations, and 28 Code of Federal Regulations Part 23.

The primary goal of this project is to back up the data already used by the RTCC to make it easier to access and visualize.

Data used by the RTCC is categorized as Law Enforcement Sensitive and will not be directly accessible by any other agency. As with any criminal investigation, information may be shared with other law enforcement agencies on an ad hoc basis, without giving the other agency direct access to the data. Under no circumstances will information be collected on individuals not related to a criminal investigation or in accordance with the City of Seattle Intelligence Ordinance.

To back up RTCC data, this project will implement the program iBase, which is a server backbone to the i2 Analyst's Notebook application currently used by SPD analysts and investigators. This server will contain some data from the Records Management System (RMS) and Computer Aided Dispatch (CAD) databases as well as supplemental information obtained during the course of criminal investigations. While this data is already accessible by RTCC staff, doing so is frequently a cumbersome and time-consuming process. iBase will allow users to visualize this data for faster access.

CAD and RMS data is the only data that will be put into the database in an automated process. Additional information, consisting of analyses, source reporting, or other investigative information not already contained in RMS and CAD, may be manually added to the iBase database, in order to provide a more complete understanding of those individuals related to criminal investigations. Manually-added information will only be entered for people directly connected to a criminal investigation.

Example of how iBase will streamline RTCC investigations:

Current System:

1) RTCC staff begin to assist an ongoing Shots Fired call where the suspect is identified but has not been found.
2) An RTCC investigator looks up the suspect in RMS, and selects the correct suspect.
3) This opens a new window with a summary of the suspect's basic information.
4) The investigator opens a separate window to see the suspect's previous addresses, which he writes down separately.
5) To see the suspect's criminal history, the RTCC staff member must open a separate window, then each incident must be opened in a separate window to see details.
6) Looking through each of the suspect's previous contacts, the investigator writes down possible associates of the suspect as well as any vehicles associated with the suspect.
7) Once all this information has been compiled in a separate document, the RTCC staff member can then relay this information to the field as possible locations where the suspect may have fled to or vehicles they may be driving.

New System:

1) RTCC staff begin to assist an ongoing Shots Fired call where the suspect is identified but has not been found.
2) An RTCC investigator looks up the suspect in iBase and selects the correct person.
3) The investigator clicks on the suspect's icon and "expands," which visualizes all previous Seattle Police law enforcement contacts as well as associated addresses, people, and vehicles linked to the suspect.
4) The investigator may also see additional information about the suspect that is not included in RMS, such as family relationships or known hangouts (manually added during previous investigations).
5) With all this information in front of him/her in just a few clicks, the RTCC staff member can relay the possible addresses and vehicles to officers in the field.

NOTIFICATION

1. ***How does the project/program provide notice about the information that is being collected?*** *Our Privacy Principles and Statement require that we provide notice to the public when we collect personal information, whenever possible.*
   - *Describe how notice will be provided to the individuals whose information is collected by this project/program and how it is adequate.*
   - *If notice is not provided, explain why not. (For certain law enforcement or other project/programs, notice may not be appropriate.)*
   - *Discuss how the notice provided corresponds to the purpose of the project/program and the stated uses of the information collected.*

   Because all the information used in this project, both automatically and manually added, is related to criminal investigations, notification to the public is not required and would impede ongoing investigations.

2. ***What opportunities are available for individuals to consent to the use of their information, decline to provide information, or opt out of the project/program?*** *Describe how an individual may provide consent for specific uses or whether consent is given to cover all uses (current or potential) of his/her information. If specific consent is permitted or required, how does the individual consent to each use? If notice is provided explain how an individual may exercise the right to consent to particular uses or decline to provide information describe the process. If this is not an option, explain why not. Note: An example of a reason to not provide an opt-out would be that the data is encrypted and therefore unlikely available to identify an individual in the event of a data breach.*

   Because all information used in this project is related to criminal investigations, individuals have no right to opt out or consent to their data being used. During the initial police contact, individuals have the option to restrict the release of their personal information as it relates to the case and this marker will be retrieved from RMS to protect the wishes of the person. All information will be stored on an encrypted server within CJIS approved environments, thus a data breach would not cause such information to be accessible.

COLLECTION

3. ***Identify the information, including personal information, that the project/program collects, uses, disseminates, or maintains.*** *Explain how the data collection ties with the purpose of the underlying mission of the department.*

Most of the data used in this project will be criminal information already available in CAD and RMS. Other data sources will include publicly available information, confidential source reporting, and databases run by other government agencies (e.g. DOL, DOC) and will be added manually based on a criminal investigation. Specific information used in this project includes:

- Basic biographical information (e.g. Name, DOB, Sex, Physical Description, etc.)
- Unique Identifiers (e.g. Driver License Numbers, Social Security Numbers, etc.)
- Contact Information (e.g. Address, Email, Phone Number)

- Photos (e.g. Booking or DOL)
- Vehicle Information
- Business Information
- Relationship Information (e.g. Parents, Siblings, Associates, etc.)
- Criminal Organization Membership (e.g. Gangs, Organized Crime)
- Event Information (e.g. crime type, location, date, etc.)

This information will only be collected on individuals related to a criminal investigation.

4. ***Is information being collected from sources other than an individual, including other IT systems, systems of records, commercial data aggregators, publicly available data and/or other departments?*** *State the source(s) and explain why information from sources other than the individual is required.*

   Information will be automatedly added from RMS/CAD and manually when directly related to a criminal investigation. No commercial data aggregators or similar technologies will be used in this project.

   Automated Input

   - **RMS and CAD** – This is the bulk of the data that will reside in iBase. Only some of the information in the current RMS and CAD systems will be added to the database (see list above). Such basic information is vital to any ongoing investigation.

   Manual Input

   - **Commercial Databases** – As part of criminal investigations, analysts and investigators already search commercial systems (e.g. Accurint, Lexis Nexis, CLEAR) for additional information on those associated with the investigation. These databases are currently accessible by law enforcement agencies, but manually adding the information to the iBase database will be useful in augmenting the information in RMS and CAD to provide a clearer understanding of the overall investigation. This data may be manually entered, but will not be automatically pulled into the database.
   - **Publicly Available Information** – As part of criminal investigations, analysts and investigators already search information that is available to any member of the public (e.g. manual Google or Twitter searches). Any criminal investigation should include information that is publicly available. This data may be manually entered, but will not be automatically pulled into the database.

USE

5. ***Describe how and why the project/program uses the information that is collected****. List each use (internal and external to the department) of the information collected or maintained. Provide a detailed response that states how and why the different data elements will be used.*

Data in this project will be used to assist in ongoing criminal investigations. Some information in the database may not be directly helpful to the investigation, but all information in the database will be related to the investigation (e.g. it may not be directly helpful to an investigation to record that the suspect wore red shoes, but recording that information is part of the investigation and may be useful for other investigations). Such uses include providing additional information on a suspect to units in the field, making connections between suspects, determining a vehicle a suspect may be driving, or determining where a suspect may live.

6. ***Does the project/program use technology to:***
    a. ***Conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly or***
    b. ***Create new information such as a score, analysis, or report?***

If so, state how the City of Seattle plans to use such results. Some project/programs perform complex analytical tasks resulting in other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Explain what will be done with the newly derived information. Will the results be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data?

Individual detectives and analysts will do nearly all the analysis of this information manually. Analysts may build networks of individuals associated with criminal cases and use simple social network analysis to identify the most influential and important members of such criminal networks. No individual will be targeted, nor will such information be added to the individual's existing record. This analysis will simply help detectives visualize the criminal networks operating around the City of Seattle.

7. ***How does the project/program ensure appropriate use of the information that is collected?*** *Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.*

There will be strict control of which users can access the data in this project (it will not be accessible by everyone within SPD). Additionally, there will be a strict audit trail that records the activity of each user within the iBase program. Information from these systems will only be shared with outside agencies manually by RTCC staff and analysts through bulletins – no other agency will have direct access to the data. SPD will conduct a regular review of audit logs to ensure proper use of the information in the system.

RETENTION

8. ***Does the project/program follow the City records retention standard for the information it collects?*** *Departments are responsible for ensuring information collected is only retained for the period required by law. City departments are further responsible for reviewing and auditing their compliance with this process. For more information, please see the internal retention schedule, here, and records retention ordinance, here.*

In addition, please provide answers to the following questions:

- *How does it dispose of the information stored at the appropriate interval?*
- *What is your audit process for ensuring the timely and appropriate disposal of information?*

Information used in this project will be retained in accordance with City of Seattle records retention standards, City of Seattle Intelligence Ordinance (when applicable), and the standards outlined in 28 CFR Part 23. One of the core project requirements specifies that the iBase software will automatically audit information based on these standards, and will notify the appropriate SPD personnel prior to record destruction. Access to the data in this project will be restricted to CJIS certified individuals who have been background checked by SPD. The data itself will be stored in compliance with CJIS requirements, including limiting physical access to the servers. In addition, SPD will conduct regular reviews of audit logs to ensure proper use and retention of the data.

SHARING

9. ***Are there other departments or agencies with assigned roles and responsibilities regarding the information that is collected?*** *Identify and list the name(s) of any departments or agencies with which the information is shared and how ownership and management of the data will be handled.*

   The information used in this project will only be directly available to SPD and assigned Seattle IT users. Products developed using this information may be shared with other law enforcement agencies. The servers and administrative tools (backup, logging, etc.) and resources (DBA's, system administrators, etc.) used for this project are subject to CJIS requirements.

10. ***Does the project/program place limitations on data sharing?***
    Describe any limitations that may be placed on external agencies further sharing the information provided by the City of Seattle. In some instances, the external agency may have a duty to share the information, for example through the information sharing environment.

    The data stored will not be accessed by an outside agency, however some products (e.g. bulletins, timelines, etc.) may be generated using the information in the database for explicit sharing with outside agencies such as other law enforcement departments when necessary for ongoing criminal investigations. This is no different from the way SPD/RTCC currently operates. All products created with the information used in this project will be classified as Law Enforcement Sensitive. They 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. The information used in this project 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. This project will abide by any new rules established in the future governing the use of data in law enforcement investigations.

11. ***What procedures are in place to determine which users may access the information and how does the project/program determine who has access?*** *Describe the process and authorization by which an individual receives access to the information held by the project/program, both electronic and paper based records. Identify users from other departments who may have access to the project/program information and under what roles these individuals have such access. Describe the different roles in*

general terms that have been created that permit access to such project/program information. Specifically, if remote access to the system is allowed or external storage or communication devices interact with the system, describe any measures in place to secure the transmission and storage of data (e.g., encryption and/or two-factor authentication).

Individual users with direct access to the iBase product will be approved on a case by case basis. Only 10 users will be allowed to access iBase at any one time, and there will be a strict audit trail of all users' actions. The project team will create processes to review the audit logs on a regular basis. Only those SPD and SeaIT CJIS certified users authorized by SPD will be allowed direct access to the data. Only law enforcement agencies will be approved recipients of RTCC products.

12. ***How does the project/program review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within City of Seattle and outside agencies?*** *Please describe the process for reviewing and updating data sharing agreements.*

    The data in the system will not be directly accessed by an outside agency. Because all the data used in this project relates to criminal investigations, any information shared will follow standard policing practices.

LEGAL OBLIGATIONS AND COMPLIANCE

13. ***Are there any specific legal authorities and/or agreements that permit and define the collection of information by the project/program in question?***
    - *List all statutory and regulatory authority that pertains to or governs the information collected by the project/program, including the authority to collect the information listed in question.*
    - *If you are relying on another department and/or agency to manage the legal or compliance authority of the information that is collected, please list those departments and authorities.*

    Information used in this project will be governed by the City of Seattle Intelligence Ordinance, 28 CFR Part 23, CJIS requirements, and any future applicable requirements.

14. ***How is data accuracy ensured?*** *Explain how the project/program checks the accuracy of the information. If a commercial data aggregator is involved describe the levels of accuracy required by the contract. If the project/program does not check for accuracy, please explain why. Describe any technical solutions, policies, or procedures focused on improving data accuracy and integrity of the project/program.*

    Sourcing of information will be an essential part of the information collection process. Most of the information coming from RMS and CAD will rely on the officers who input the information to ensure its accuracy. RTCC staff and analysts will check the accuracy of information as individual incidents are reviewed regularly. No data aggregators or other automated programs will be used to input information outside of RMS and CAD. Any additional information will be manually reviewed at the time it is added to the system.

15. ***What are the procedures that allow individuals to access their information?***

Describe any procedures or regulations the department has in place that allow access to information collected by the system or project/program and/or to an accounting of disclosures of that information.

The information used in this project 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.

16. ***What procedures, if any, are in place to allow an individual to correct inaccurate or erroneous information?*** *Discuss the procedures for individuals to address possibly inaccurate or erroneous information. If none exist, please state why.*

    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. If an individual believes SPD's data about them is incorrect, they may follow the same procedures they would for all other data in SPD's systems.

17. ***Is the system compliant with all appropriate City of Seattle and other appropriate regulations and requirements?*** *Please provide details about reviews and other means of ensuring systems and project/program compliance.*

    This system fully complies with city, state, and federal regulations. SPD will conduct regular reviews of audit logs to ensure proper compliance with such regulations.

18. ***Has a system security plan been completed for the information system(s) supporting the project/program?*** *Please provide details about how the information and system are secured against unauthorized access.*

    The security plan will be developed with the assistance of the vendor when the system is built. The servers will reside on the SPD network and Seattle IT will manage system security and access in compliance with CJIS requirements

19. ***How is the project/program mitigating privacy risk? G****iven the specific data elements collected, discuss 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 primary privacy risk with this project pertains to information being added on individuals not directly associated with criminal activity. To mitigate this risk, users will only add information on individuals when they are associated with a criminal investigation and/or collected in accordance with the City of Seattle Intelligence Ordinance. In addition, SPD will conduct regular reviews of audit logs to ensure proper use and retention of the data.

MONITORING AND ENFORCEMENT

20. ***Describe how the project/program maintains a record of any disclosures outside of the department.*** *A project/program may keep a paper or electronic record of the date, nature, and purpose of each disclosure, and name and address of the individual or agency to whom the disclosure is made. If the project/program keeps a record, list what information is retained as part of the accounting requirement. A separate system does not need to be created to meet the accounting requirement, but the project/program must be able to recreate the information noted above to demonstrate compliance. If the project/program does not, explain why not.*

    These systems will not be directly accessed by outside agencies. Information may be shared with outside agencies as it would with any criminal investigation. Any bulletins or other notifications created with information or analysis resulting from this project will be kept in the SPD network file system as well as recorded in the established SPD bulletin system.

21. ***Have access controls been implemented and are audit logs are regularly reviewed to ensure appropriate sharing outside of the department?*** *Is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies? Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.*

    Audit logs track all users' activity within the iBase system. No users outside SPD will have direct access to the system. Only those SPD and SeaIT CJIS certified users authorized by SPD will be allowed direct access to the data.

22. ***How does the project/program ensure that the information is used in accordance with stated practices of the project/program?*** *What auditing measures are in place to safeguard the information and policies that pertain to them? Explain whether the project/program conducts self-audits, third party audits or reviews.?*

    All RTCC staff and analysts undergo training before gaining access to RTCC systems. Only a select number of officers and analysts will be granted access to the RTCC. The iBase system requires additional training before users will be granted an account.

23. ***Describe what privacy training is provided to users either generally or specifically relevant to the project/program.*** *City of Seattle offers privacy and security training. Each project/program may offer training specific to the project/program, which touches on information handling procedures and sensitivity of information. Discuss how individuals who have access to personal information are trained to handle it appropriately. Explain what controls are in place to ensure that users of the system have completed training relevant to the project/program.*

    All RTCC personnel will undergo the following privacy and security trainings:

    - CJIS Certification
    - Online Privacy Security Training
    - All relevant SPD training and directives
    - Individual iBase training (to be developed in-house).

24. ***Is there any aspect of the project/program that might cause concern by giving the appearance to the public of privacy intrusion or misuse of personal information?*** *Examples might include a push of information out to individuals that is unexpected and appears to be intrusive, or an engagement with a third party to use information derived from the data collected that is not explained in the initial notification.*

    The public may express concern over the consolidation of so much information about individuals, but all the data that will be 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 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 information on people with no connection to criminal investigations or related to Seattle Police response to an incident.