2025 Privacy Impact Assessment

Forcemetrics

Seattle Police Department

1/29/2025

Contents

Privacy Impact Assessment Overview

What is a Privacy Impact Assessment?

A Privacy Impact Assessment ("PIA") is an analysis of how personal data is gathered, processed, and used for a particular program, project, data initiative, or technology implementation (the terms may collectively be referred to hereafter as "effort"). The PIA asks questions about the collection, use, sharing, security and access of data involved in a City department effort. It also requests information about policies, training and documentation that govern use of the data and any associated technology. The PIA responses are used to determine privacy risks and mitigation measures to reduce those risks. To ensure transparency about personal 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 PIA required?

A PIA may be required when a project, program, or other data processing activity has been flagged through the privacy review process as having a high privacy risk.

How to complete this document?

As department staff complete the document, they should keep the following in mind.

- Department Subject Matter Experts (SME) are responsible for providing responses to the questions. *Please do not edit the questions or question descriptions that are part of the template.*
- All content in this report will eventually be published to the public. Therefore, avoid using acronyms, slang, or other terms which may not be well-known to external audiences. Additionally, responses should be written principally using non-technical language to ensure they are understood by audiences unfamiliar with the topic.

1.0 Overview

1.1 Description: Please describe the effort.

Include high level descriptions of any technology and its intended use, the data collected or processed, and all third parties involved in the effort.

ForceMetrics provides law enforcement entities feature enriched visualizations of public safety data, and data linkage from multiple existing data sources related to community impact, operational efficiencies, and performance metrics to identify community needs, measure success and mitigate risks, and Standard Support Services. ForceMetrics will never be used to label or identify a person, it is used only to tag an incident.

This web-based application will enable the Seattle Police Department to more easily search for and review unstructured data contained in Computer-Aided Dispatch (CAD) and Mark43, our Records Management System (RMS). ForceMetrics does not search any external data, including online or social media.

1.2 Business Need: What business need/problem does this effort address?

Please describe why the department is undertaking this effort.

ForceMetrics will provide SPD "feature enriched" visualizations of public safety data and data linkage from multiple approved and existing data sources related to community impact, operational efficiencies, and performance metrics in order to identify community needs, measure success and mitigate risks and Standard Support Services. SPD will use ForceMetrics to assist with the analysis of key programs such as Missing and Murdered Indigenous People (MMIP) as well as others. This effort is in line with Seattle City Council Resolution 31900 as it supports better understanding around the scope of the data issues related to the efforts around Missing and Murdered Indigenous Women and Girls (MMIWG).

Identified use cases are:

1) Utilizing ForceMetrics to enhance awareness and understanding of the "Urban Indian" population (i.e., tribal/indigenous involvement) through existing data collected by SPD.

By leveraging ForceMetrics' data analytics and enrichment capabilities, SPD can identify service delivery (based on reports), involving indigenous/Urban Indian people. This enables SPD to develop more culturally sensitive approaches to community engagement, law enforcement, and public safety, thereby fostering positive relationships and outcomes with the Indigenous community (trust, accountability and perceptions of legitimacy).

2) Utilizing ForceMetrics to enhance public safety needs assessment and evaluation of events at the intersection of police service and the housing crisis (homelessness).

By leveraging ForceMetrics' data analytics and enrichment capabilities, SPD can identify events involving unhoused/unsheltered people from the myriad ways they can appear in written reports. This proactive approach enhances community safety, promotes collaboration with relevant service providers, and supports individuals in accessing the necessary resources to address their specific circumstances, ultimately working toward reducing harm and improving community outcomes.

1.3 Benefits: What are the anticipated benefits of this effort and how does it relate to departmental and/or City mission?

What is the intended outcome, goal, or benefit? Please provide any data or research demonstrating the anticipated benefits of the effort (e.g. academic studies, etc.).

By providing comprehensive data and insights, ForceMetrics ensures that employees' actions comply with law and policy, conduct thorough investigations, and recommend policy improvements. The platform provides contextual search capabilities, which will assist with investigations and ensure a wholistic approach to policing.

1.4 Technology Details: Describe all technologies that support or will be used as part of the effort.

What systems interact with the data involved in this effort? This includes hardware and software throughout the data lifecycle (e.g. creation, collection, use, storage, disclosure, and destruction). Describe, by name and functionality, all technologies associated with the effort. For example: high-level Microsoft Forms to collect the data, Microsoft Excel to extract the data.

ForceMetrics is a web application that enables the Seattle Police Department to more easily search for and review data stored in Computer-Aided Dispatch (CAD) and Mark43. ForceMetrics does not search any external data, including online or social media.

1.5 Scope of Involvement & Use: Who is involved in the implementation or use of the technology, project, and associated data?

For example, what other departments, if any, are involved? Are external partners (e.g. community-based organizations) or vendors/consultants involved?

Only authorized users will have access to ForceMetrics and access to the application will be limited to SPD personnel via password-protected login credentials. 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. SPD will conduct a regular review of audit logs to ensure proper use of the information in the system. Current scope of authorization includes research and evaluation, no operational purpose (investigation of a specific crime, prosecution of a specific person, etc.) is authorized under this assessment. If and when the SPD determines the technology to be safe, based on a sufficient understanding of risks, benefits and potential countermeasures, additional authorization for expanded use may be sought.

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.

2.0 Data Details & Collection Practices

2.1 Data Subjects: Whose data will be collected or processed as part of this effort?

Please provide all categories of data subjects (e.g., members of the public, City employees, contractors, etc.) as well as any sub-populations that might be involved (e.g., children, older adults/elderly, incarcerated or formerly incarcerated persons, unhoused persons, etc.)

ForceMetrics only uses data already collected from existing and authorized SPD data sources. It does not collect data from outside sources that are not already held by SPD systems. ForceMetrics does not search any external data, including online or social media.

Data stored in Computer-Aided Dispatch (CAD) and Mark43 are all in response to a law enforcement contact –which include members of the public, city employees, and others.

2.2 Data Fields: What are the data fields and data types that are involved in this effort?

Please describe all data collected, stored, generated, analyzed, used, and/or shared, etc.

ForceMetrics will have access to data associated with an SPD call for service or self-initiated activity. Fields and data type are dependent on what is captured in the Computer-Aided Dispatch (CAD) and Mark43. Personal data, including individual PII and criminal history information related to all individuals whose data is in SPD data systems. ForceMetrics does not search any external data, including online or social media.

2.3 Data Collection: How is the data collected for this effort? What are the data sources for the data used or processed as part of this effort?

Please describe the methods of data collection (e.g., first-party collection which is collection directly from an individual; third-party collection which is collection through another entity, etc.). Also include the mechanism by which the data is collected (e.g., online form/survey, data purchase, data shared/provided by another department, etc.).

ForceMetrics will not be collecting any data. ForceMetrics will process data from existing and approved City systems, primarily the Computer-Aided Dispatch (CAD) and the Records Management System (RMS). ForceMetrics does not collect data from outside sources that are not already held by SPD systems. Data stored in Computer-Aided Dispatch (CAD) and Mark43 are all in response to a law enforcement contact and serve a law enforcement purpose, primarily.

2.4 Data Flow: Describe how data collected flows through the data lifecycle including the assets used to store and process the data. ("Assets" are things that support the information-related activities, such as software systems, appliances, databases, etc.)

In other words, after data is obtained, where will it go? Where will it spend most of its time? Will it stay put, or will it go somewhere else?

ForceMetrics will not be collecting any data. ForceMetrics will process data from existing and approved City systems, primarily the Computer-Aided Dispatch (CAD) and the Records Management System (RMS). ForceMetrics does not collect data from outside sources that are not already held by SPD

systems. Data stored in Computer-Aided Dispatch (CAD) and Mark43 are all in response to a law enforcement contact and serve a law enforcement purpose, primarily.

2.5 Notice: At the point of data collection, how are individuals notified about the City's use, sharing, and disclosure of their personal data?

Please include all methods, processes, or mechanisms for notification. This may include the City's standard disclosure, use, and sharing notice.

No notification will be provided.

ForceMetrics will not be collecting any data. ForceMetrics will process data from existing and approved City systems, primarily the Computer-Aided Dispatch (CAD) and the Records Management System (RMS). ForceMetrics does not collect data from outside sources that are not already held by SPD systems. Data stored in Computer-Aided Dispatch (CAD) and Mark43 are all in response to a law enforcement contact and serve a law enforcement purpose, primarily.

3.0 Data Use & Processing

3.1 Authorized Data Uses: What are the authorized uses of the data associated with this effort?

In addition to describing all authorized uses of the data, list any data use limitations and unauthorized data uses.

Only authorized SPD users can access ForceMetrics or data. Access to the application will be limited to SPD personnel via password-protected login credentials. In accordance with CJIS policy and security requirements.

SPD will use ForceMetrics in accordance with the approved scope defined in question 1.1 and 1.2 (see below).

1) Utilizing ForceMetrics to enhance awareness and understanding of the "Urban Indian" population (i.e., tribal/indigenous involvement) through existing data collected by SPD.

By leveraging ForceMetrics' data analytics and enrichment capabilities, SPD can identify service delivery (based on reports), involving indigenous/Urban Indian people. This enables SPD to develop more culturally sensitive approaches to community engagement, law enforcement, and public safety, thereby fostering positive relationships and outcomes with the Indigenous community (trust, accountability and perceptions of legitimacy).

2) Utilizing ForceMetrics to enhance public safety needs assessment and evaluation of events at the intersection of police service and the housing crisis (homelessness).

By leveraging ForceMetrics' data analytics and enrichment capabilities, SPD can identify events involving unhoused/unsheltered people from the myriad ways they can appear in written reports. This proactive approach enhances community safety, promotes collaboration with relevant service providers, and supports individuals in accessing the necessary resources to address their specific circumstances, ultimately working toward reducing harm and improving community outcomes.

3.2 Authorized Technology Uses: What are the authorized use cases for the technology associated with this effort? How may the technology be used?

In addition to describing all authorized use cases for the technology, list any technology use limitations and unauthorized technology uses.

Some use cases for ForceMetrics relate to resource management, safety signal alerts, and enhanced community relations. With respect to resource management, consolidating critical information from various databases, ForceMetrics allows SPD to allocate resources more efficiently, ensuring that officers have the information they need when they need it. Finally, by recognizing patterns and identifying key markers, ForceMetrics can help officers address community-specific issues more proactively, leading to better police-community relations.

3.3 Use & Management Policies: What policies (City or department-specific) apply to the use and management of the data *and* technology (if different than the data) associated with this effort?

Please name and describe all applicable policies.

Only authorized users will have access to ForceMetrics and access to the application will be limited to SPD personnel via password-protected login credentials. 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 trial that records the activity of each user. SPD will conduct a regular review of audit logs to ensure proper use of the information in the system. 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.

3.4 Data Processing & Analytics: Please describe how the data will be processed and analyzed in support of the intended business goal/outcome. Please include metrics.

Describe the scale of processing and analysis to the best of your ability, as well as whether analysis involves matching or combining datasets. Describe the fields required for joining, and the metrics the business will use for the analysis.

ForceMetrics will provide SPD with feature enriched visualizations of public safety data and data linkage from multiple existing data sources related to community impact, operational efficiencies, and performance metrics in order to identify community needs, measure success and mitigate risks and Standard Support Services. SPD will use ForceMetrics tags to assist with the analysis of key programs such as Missing and Murdered Indigenous People (MMIP) as well as others.

Only authorized SPD users can access ForceMetrics or data. Access to the application will be limited to SPD personnel via password-protected login credentials. In accordance with CJIS policy and security requirements.

4.0 Legal Scope & Compliance

4.1 Governing Laws: What laws, regulations, rules, or contracts govern (a) the data, (b) the data processing activities, (c) the data sharing?

ForceMetrics only uses data compiled from existing SPD data sources. It does not collect data from outside sources that are not already held by SPD systems. Only authorized SPD users can access ForceMetrics. Access to the application will be limited to SPD personnel via password-protected login credentials. Additionally, 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. Finally, the implementation and use of ForceMetrics supports City Council Resolution 31900.

4.2 Compliance Measures: What are the compliance measures associated with the use of the technology or data? Who is involved with oversight of requirements defined in 4.1?

Please explain any departmental, City, and/or third-party oversight.

Only authorized SPD users can access Forcemetrics or data. Access to the application will be limited to SPD personnel via password-protected login credentials. 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.

4.3 Records Production Compliance: How is the data and/or associated records (e.g., reports, derivatives, etc.) retrievable in support of public disclosure requirements?

Please describe the method and process for extracting/retrieving/producing the data.

Per RCW 42.56.070, the Department must make all public records available to a requester, unless the record falls within the specific exemptions in the Public Records Act (PRA) or other statute which exempts or prohibits disclosure of specific information or records.

5.0 Data Security, Protection, & Storage

5.1 Data Access: Who will have access to the data? Who will have access to the technology (if different than who has data access)?

Only authorized users will have access to ForceMetrics and access to the application will be limited to SPD personnel via password-protected login credentials. 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 trial that records the activity of each user. SPD will conduct a regular review of audit logs to ensure proper use of the information in the system.

5.2 Access Authorization: What processes are prerequisites to a user's access of the data or technology (e.g., user authentication, business approvals/sign-off, documentation, etc.)?

As part of your response, include who (by City title) is responsible for authorizing data access.

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.

5.3 Secure Storage: Where will the data be stored, and what security measures are in place for the storage of the data?

AWS stores data in geographically distinct regions around the world. AWS GovCloud consists of two physically and logically isolated regions in the United States, ensuring data remains within the country and complies with various stringent U.S. government security and compliance requirements, such as the FBI's Criminal Justice Information Services (CJIS). No data will be stored and/or retained on premise.

5.4 Auditability of Data Access & Data Processing: How will the department ensure that data access and data processing activities are logged and auditable?

This could be conducted manually (e.g., business process), by technology/technical functionality, or a combination of both.

SPD's Audit, Policy and Research Section (APRS) can conduct an audit of any and all systems at any time. In addition, the Office of Inspector General and the federal monitor can access all data and audit for compliance at any time.

6.0 Data Sharing & Disclosure

6.1 Data Sharing Partners: Which entities (internal and external to the City) will be data sharing partners, if any?

Please describe all parties that will have access to both the data and data derivatives (including other City departments).

ForceMetrics will not share any data with agencies, third parties, or other entities without an executed MOU between agencies. Additionally, the data stored will not be accessed by an outside agency. Data within ForceMetrics may be shared outside SPD with other agencies, entities, or individuals within legal guidelines or as required by law.

6.2 Purpose for Data Sharing: What is the purpose of sharing data with the identified parties in the context of this effort?

Data sharing may be necessary for SPD to fulfill its mission of contributing to crime reduction by assisting in collecting evidence related to serious and/or violent criminal activity as part of investigation, and to comply with legal requirements. Additionally, SPD shares data with authorized researchers pursuant to properly execute research and confidentiality agreements as provided by SPD Policy 12.055.

This sharing may include discrete pieces of data related to specific investigative files collected via CAD and Mark43.

6.3 Sharing Restrictions: Describe any restrictions on data use and data access and identify the sources that impose those restrictions.

Data sharing agreements/contracts, department policies and procedures, department rules, laws, regulations, and other authorities may impose data restrictions.

Research agreements must meet the standards reflected in **SPD Policy 12.055**. Law enforcement agencies receiving criminal history information are subject to the requirements of **28 CFR Part 20**. In addition, Washington State law enforcement agencies are subject to the provisions of **WAC 446-20-260**, and **RCW Chapter 10.97**.

6.4 Agreement Updates: Please describe the process for reviewing and updating data sharing agreements.

Please describe the processes for initial development, agreement review, new uses of the data, and new access to the data (including internal and external to the City) as well as how often the agreement gets updated.

First, Research Agreements must meet the standards reflected in SPD Policy 12.055. When engaging in a Research Agreement, the SPD agrees to provide Researcher(s) access and information only as outlined by the Research Agreement. The parties anticipate that a need for access, data or information not mentioned below may appear as the research continues. The Researcher may request additional data, access or information in writing and the Research Agreement may be modified to permit the SPD to provide such additional data, access or information.

6.5 Records of Data Disclosure: How are records that document data disclosure/sharing maintained by the department?

Please describe how these records are documented either by technical functionality or business practices/processes.

SPD's Audit, Policy and Research Section (APRS) can conduct an audit of the any and all systems at any time. In addition, the Office of Inspector General and the federal monitor can access all data and audit for compliance at any time. Audit data is available to the public via Public Records Request.

7.0 Data Retention & Destruction

7.1 Data Retention: What are the record retention schedules that govern both the raw data and any derived outputs (e.g., analyses, reports, transformed/cleaned datasets)?

ForceMetrics does not retain data. However, data from CAD/RMS is 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. Access to the data is 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.

Analysis of tags identified by ForceMetrics are done in other platforms and this software only tags data in order to be further used downstream. For any occasion in which outputs from ForceMetrics are used to inform policies, reports or recommendations the analysis will be available in accordance with public records laws.

7.2 Data Destruction: What mechanisms (technical or process-oriented) are in place to destroy improperly collected data?

ForceMetrics will not be collecting any data. However, SPD policy contains multiple provisions to avoid improperly collecting data. 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.

7.3 Responsible Staff: Who is responsible for ensuring compliance with data retention and data destruction requirements?

Please respond with City title(s)/roles only.

ForceMetrics will not be collecting any data. However, SPD policy outlines that unit supervisors are responsible for ensuring compliance with data retention 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.

7.4 Purge Verification: What mechanisms (technical or process-oriented) are in place to ensure that data is properly destroyed after data retention periods have been met?

ForceMetrics will not be collecting any data.

8.0 Privacy Principles, Risks, & Controls

The City's Privacy Program staff will help in completing this section.

8.1 Privacy Risks, Harms, Mitigations, & Controls: What privacy risks exist for the effort, and what are the potential impacts on Seattle residents and/or other data subjects?

What are the controls or mitigations that are in place to address these risks, and reduce the likelihood that unintended harms are realized?

Risk: Sensitive data in RMS and CAD used in new AI software may introduce additional security risks that could impact individuals' personal data.

Mitigation/Control: Ensure security protections are in place. The protections implemented to address this risk include: Single Sign-on (SSO), Role-based access controls, audit logs, and two factor authentication. Additionally, the solution is hosted in AWS Government Cloud, and therefore meets AWS Government Cloud Security standards. The cloud environment meets CJIS compliance and security standards. Finally, CJIS data is regulated and, in some cases, protected under law.

Risk: Each data element, depending on the sensitivity and data classification, should only be processed or used after evaluation and determination of need for each field identified. Risk includes overuse of previously collected data, beyond the scope of defined use cases reflected in the PIA.

Mitigation/Control: SPD has evaluated the exact purpose for which each data element is needed and protected in accordance with applicable laws and best practices. No new data is collected specifically for use of ForceMetrics. The approved use cases are scoped as outlined in this Privacy Impact Assessment.

AI Risk: Downstream decisions impacting SPD services resulting from AI use (for example: inaccuracies in model outputs/tags may impact insights or service decisions downstream). This could impact certain populations or groups, depending on how the AI system applies tags, may result in unintentional perpetuation of systemic bias as a result of AI system outputs; however, the authorized scope of this implementation is intended to improve visibility and response to historically underserved communities.

Mitigation/Control: SPD will be actively involved in the development and implementation of AI based data enrichment (NLP tagging). In addition to fundamental methodological controls, system accuracy and performance will be actively monitored to assure minimum performance thresholds, as defined by the department, are maintained. Analysts will validate tag accuracy and will actively provide feedback to improve accuracy. The system uses natural language processing to tag incidents and not people. Tag categories are broad and are produced for analytical purposes only. No data will be written back to the system of record (CAD and/or RMS) based on ForceMetrics automated feature enrichment (i.e., tagging). Certain labels related to vulnerable populations will not be activated (i.e., immigration status), unless expressly authorized under a new PIA.

AI Risk: Sensitive information disclosure through use of AI system models, based on ingestion of sensitive data held by the City.

Mitigation/Control: Contractual requirements are in place to ensure City data will not be used to train or fine-tune the commercial product.