2020 Surveillance Impact Report

Video Recording Systems

(Interview, Blood-Alcohol Collection Room, and Precinct Holding Cell Audio)

Seattle Police Department

Seattle Information Technology

DRAFT

Surveillance Impact Report ("SIR") Overview

About the Surveillance Ordinance

The Seattle City Council passed ordinance 125376, also referred to as the "Surveillance Ordinance", on September 1, 2017. This ordinance has implications for the acquisition of new technologies by the City, and technologies that are already in use that may fall under the new, broader definition of surveillance.

SMC 14.18.020.B.1 charges the City's executive with developing a process to identify surveillance technologies subject to the ordinance. Seattle IT, on behalf of the executive, developed and implemented a process through which a privacy and surveillance review is completed prior to the acquisition of new technologies. This requirement, and the criteria used in the review process, are documented in Seattle IT Policy PR-02, the "Surveillance Policy".

Surveillance Ordinance Review Process

The following is a high-level outline of the complete SIR review process.

Upcoming for Review	Initial Draft	Open Comment Period	Final Draft	Working Group	Council Review
The technology is upcoming for review, but the department has not begun drafting the surveillance impact report (SIR).	Work on the initial draft of the SIR is currently underway.	The initial draft of the SIR and supporting materials have been released for public review and comment. During this time, one or more public meetings will take place to solicit feedback.	During this stage the SIR, including collection of all public comments related to the specific technology, is being compiled and finalized.	The surveillance advisory working group will review each SIR's final draft and complete a civil liberties and privacy assessment, which will then be included with the SIR and submitted to Council.	City Council will decide on the use of the surveillance technology, by full Council vote.

DRAFT

Privacy Impact Assessment

Purpose

A Privacy Impact Assessment ("PIA") is a method for collecting and documenting detailed information collected in order to conduct an in-depth privacy review of a program or project. A PIA asks questions about the collection, use, sharing, security and access controls for data that is gathered using a technology or program. It also requests information about policies, training and documentation that govern use of the technology. The PIA responses are used to determine privacy risks associated with a project and mitigations that may reduce some or all of those risks. In the interests of transparency about 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 Privacy Impact Assessment Required?

A PIA may be required in two circumstances.

1) When a project, technology, or other review has been flagged as having a high privacy risk.
2) When a technology is required to complete the surveillance impact report process. This is one deliverable that comprises the report.

1.0 Abstract

1.1 Please provide a brief description (one paragraph) of the purpose and proposed use of the project/technology.

SPD has two camera systems used to record and/or monitor members of the public within specific, secure locations in SPD facilities.

The first is the Genetec Video Management System. It is a permanently installed, non-mobile unconcealed audio and video recording system primarily used to record in-person interactions with and interviews of crime victims, witnesses, and suspects in 7 designated interview rooms located at the SPD headquarters in the Seattle Justice Center. The system also provides a live video-only view of these interview rooms. The video-only live view is used to monitor, short term, members of the community who are in the interview rooms when no SPD detective is present. This system is used to create a video record of interviews for the purposes of use in criminal justice proceedings.

The second is Milestone Systems XProtect Video Management Software and Products. These are permanently installed in SPD's Blood Alcohol Collection (BAC) rooms and precinct holding cells. They record continuously all activity in those locations.

DRAFT

1.2 Explain the reason the project/technology is being created or updated and why the PIA is required.

These technologies are used to record members of the public who are being interviewed or having their blood alcohol levels tested or are placed in precinct holding cells. If used out of policy, improperly, or without proper notification, this technology could potentially be used to make recordings that infringe on public privacy.

2.0 Project / Technology Overview

Provide an overview of the project or technology. The overview gives the context and background necessary to understand the purpose, mission and justification for the project / technology proposed

2.1 Describe the benefits of the project/technology.

Though the state of Washington is not one of the 26 states that requires the recording of custodial interrogations, many law enforcement agencies and criminal justice system watchdogs, such as the Innocence Project, highly recommend the practice. Benefits include: preventing disputes about how an officer conducted the interview or treated a suspect or victim; creating a record of statements made by a suspect that may capture subtle details missed in real-time; reducing false confessions; and enhancing public confidence in the practices of SPD. Creating a visual record of activities that occur within the BAC rooms and precinct holding cells also provides a measure of accountability for both SPD and involved community members.

2.2 Provide any data or research demonstrating anticipated benefits.

According to The Justice Project, "the virtue of electronic recording of custodial interrogations… lies not only in its ability to help guard against false confessions, but also in its ability to develop the strongest evidence possible to help convict the guilty." (https://web.williams.edu/Psychology/Faculty/Kassin/files/Justice%20Project(07).pdf)

2.3 Describe the technology involved.

The Genetec Video Management System includes camera and microphone equipment that is permanently installed in the interview rooms on the 6th and 7th floors of SPD Headquarters, a physical server located at SPD HQ, two dedicated computer workstations located in the detectives' work area at SPD HQ, and video-only monitors located throughout the detectives' work area and detective supervisors' offices at SPD HQ.

The Milestone Video Management Software and Products consist of cameras located in BAC rooms and precinct holding cells throughout SPD's facilities. A dedicated server is located at each of these secure locations which stores the video and audio information from the Milestone cameras.

DRAFT

2.4 Describe how the project or use of technology relates to the department's mission.

The mission of the Seattle Police Department is to prevent crime, enforce the law, and support quality public safety by delivering respectful, professional, and dependable police services. The video and audio recording of victim, witness, and suspect interviews aids investigations and prosecutions of crimes as well as enhances public confidence in the practices of SPD.

2.5 Who will be involved with the deployment and use of the project / technology?

All SPD investigative units which include: Homicide, Robbery, Gang Unit, Intelligence, Special Assault Unit, Domestic Violence Unit, Arson-Bomb Squad, Major Crimes, Auto Theft, Vice & Human Trafficking. All SPD precinct employees tasked with the collection of blood alcohol levels and holding of subjects in precinct holding cells.

Additionally, SPD Video Unit staff, and certain backgrounded and qualified Seattle IT personnel are also involved in the support of the Video Management Systems.

3.0 Use Governance

Provide an outline of any rules that will govern the use of the project / technology. Please note: non-City entities contracting with the City are bound by restrictions specified in the surveillance ordinance and privacy principles and must provide written procedures for how the entity will comply with any restrictions identified.

DRAFT

3.1 Describe the processes that are required prior to each use, or access to/ of the project / technology, such as a notification, or check-in, check-out of equipment.

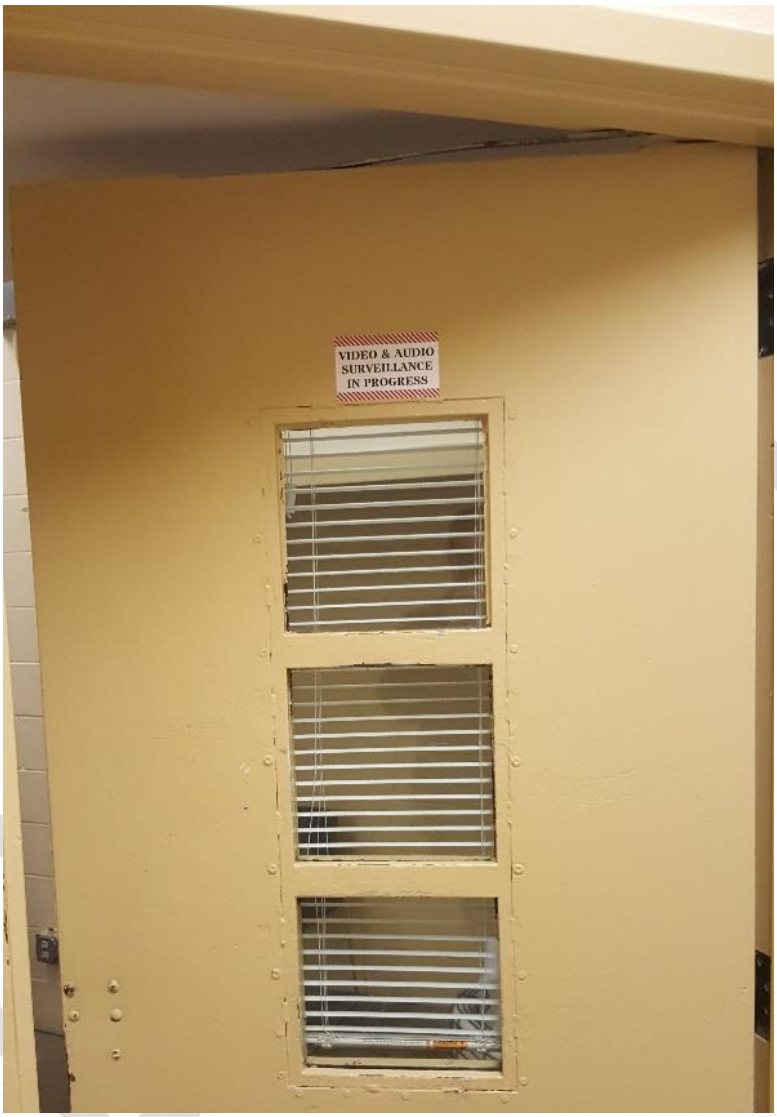
Genetec (Interview rooms): The detective(s) conducting the interview activates the recording system for the appropriate room with a manual switch. The detective then advises the interview subject of the audio recording acquiring implied consent, or explicitly asks for permission to record per SPD Policy 7.110 – Recorded Statements. At the conclusion of the interview or blood draw, or when the subject leaves the room, the recording is terminated by the detective or officer. The detective then exports the recording from the server on one of the two designated computer work stations and creates a copy of the recording for permanent storage on a special high-quality evidence grade DVD+R disc. This evidence grade disc is then submitted into the SPD Evidence Section as a standard item of evidence.

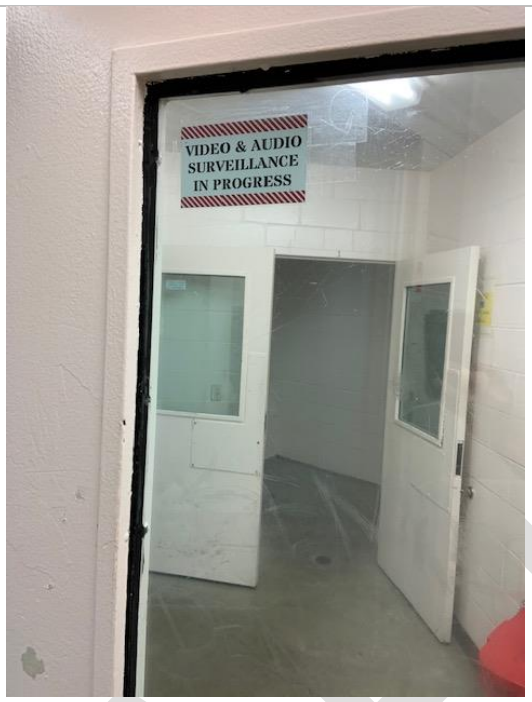
Milestone (BAC rooms and precinct holding cells): The Milestone systems is continuously recording in the BAC rooms and precinct holding cells. In the event that an investigator (including SPD internal investigations) needs to view the video, a request must be made to the SPD Video Unit who will locate the specific time and location video requested and provide the investigator with a DVD containing the file.

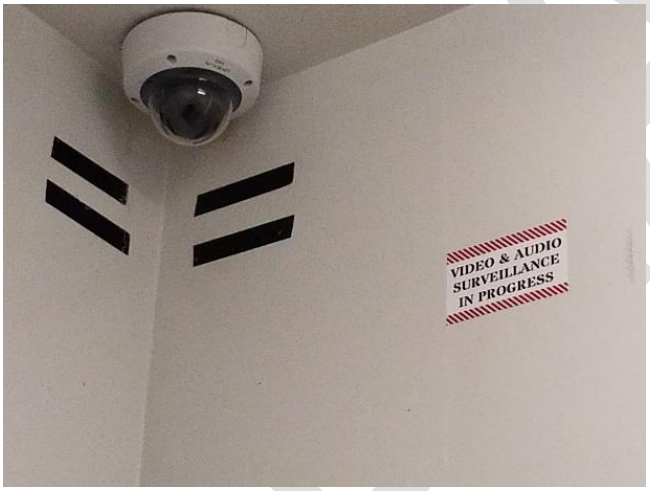
3.2 List the legal standards or conditions, if any, that must be met before the project / technology is used.

DRAFT

Signage is clearly posted in all SPD precincts indicating that audio and video surveillance is in progress. These signs are posted both at the entrances to holding cells and inside holding cells and blood alcohol collection areas.







Consent is required before these technologies may be used. **RCW 9.73.030 Intercepting, recording or divulging private communication – Consent required – Exceptions.** Also known as "All party consent". Standard procedure dictates that interview subjects are always advised of the presence of the recording or asked for their permission to record. Any recording made of an interview subject without consent would be inadmissible and could possibly subject the SPD personnel to an internal conduct assessment and possibly criminal charges.

Per SPD Policy 7.110 – Recorded Statements:

When taking an audio recorded statement, the officer/detective:

1. **States** at the beginning of the recording:

   Officer's name and includes, "of the Seattle Police Department"
   Report Number
   Date and time of the recording
   The name of the interviewee
   All persons present during the interview

2. **Asks** the person to respond to the question, "Are you aware you are being recorded?"

3. **If** the person is in custody, **gives** Miranda warning.

4. **Asks** the person to state their full name.

5. **Conducts** the interview.

6. After the interview, **if** the person is a victim, witness or complainant, **asks** the person:

   Do you declare under penalty of perjury under the laws of Washington what you have stated in this statement is true and correct?
   Do you wish to have your personal information Disclosed or Not Disclosed?

7. **Announces** the end of the recording with the date and time.

8. **Uploads** the audio statement to the Digital Evidence Management System (DEMS).

9. **Documents** the recorded statement in the appropriate report.

DRAFT

3.3 Describe the policies and training required of all personnel operating the project / technology, and who has access to ensure compliance with use and management policies.

Operators of both the Genetec and Milestone video systems are sworn SPD personnel. Training on the use of these systems is provided in-house to all SPD users of this technology. All SPD employees are required to abide by all SPD policies, including SPD Policy 7.110 – Recorded Statements which is directly related to the use of video recording equipment.

4.0 Data Collection and Use

Provide information about the policies and practices around the collection and use of the data collected.

4.1 Provide details about what information is being collected from sources other than an individual, including other IT systems, systems of record, commercial data aggregators, publicly available data and/or other City departments.

These technologies record only the images and sounds that occur during an SPD interview of a witness, victim, or suspect, and activity in BAC rooms and precinct holding cells.

4.2 What measures are in place to minimize inadvertent or improper collection of data?

These technologies record only the images and sounds that occur during an SPD interview of a witness, victim, or suspect, and activity in BAC rooms and precinct holding cells. These technologies are permanently mounted and do not record any information outside of these parameters.

4.3 How and when will the project / technology be deployed or used? By whom? Who will determine when the project / technology is deployed and used?

Genetec (Interview rooms): The detective(s) conducting the interview activates the recording system for the appropriate room with a manual switch. The detective then advises the interview subject of the audio recording acquiring implied consent, or explicitly asks for permission to record per SPD Policy 7.110 – Recorded Statements. At the conclusion of the interview or blood draw, or when the subject leaves the room, the recording is terminated by the detective or officer. The detective then exports the recording from the server on one of the two designated computer workstations and creates a copy of the recording for permanent storage on a special high-quality evidence grade DVD+R disc. This evidence grade disc is then submitted into the SPD Evidence Section as a standard item of evidence.

Milestone (BAC rooms and precinct holding cells): The Milestone systems is continuously recording in the BAC rooms and precinct holding cells. In the event that an investigation (including SPD internal investigations) needs to view the video, a request must be made to the SPD Video Unit who will locate the specific time and location video requested and provide the investigator with a DVD containing the file.

4.4 How often will the technology be in operation?

The Genetec (interview rooms) system is used on a daily basis in the course of law enforcement activities. The Milestone system (BAC rooms and precinct holding cells) records these locations continuously.

DRAFT

4.5 What is the permanence of the installation? Is it installed permanently, or temporarily?

Both the Genetec and Milestone systems are permanently installed.

4.6 Is a physical object collecting data or images visible to the public? What are the markings to indicate that it is in use? What signage is used to determine department ownership and contact information?

The cameras for both the Genetec and Milestone systems are overtly mounted in the interview rooms at SPD Headquarters and inside BAC rooms and precinct holding cells.

4.7 How will data that is collected be accessed and by whom?

Genetec (interview rooms): After an interview is conducted, the detective accesses the recorded audio-video file that is stored on the Genetec server using proprietary Genetec software on one of two dedicated workstations located in the secured Detectives' Working Area and creates a copy of this file on a high-quality evidence grade DVD+R disc. This evidence-grade disc is then submitted into the SPD Evidence Section as a standard item of evidence. Standard evidence retention/disposition rules are then followed.

Milestone (BAC rooms and precinct holding cells): The recordings made by the Milestone system of BAC room use is not accessed routinely, but rather only when a specific request for that footage is needed for a criminal or internal investigation. Requests for that footage is requested by an authorized party (detective, Office of Police Accountability investigator, etc.) to the SPD Video Unit within the 90-day data retention period for those files. The Video Unit creates a copy of this file on a high-quality evidence grade DVD+R disc. This evidence grade disc is then submitted into the SPD Evidence Section as a standard item of evidence. Standard evidence retention/disposition rules are then followed.

4.8 If operated or used by another entity on behalf of the City, provide details about access, and applicable protocols.

This technology is not operated or used by another entity on behalf of the City.

4.9 What are acceptable reasons for access to the equipment and/or data collected?

The primary reason for access to the data collected by both the Genetec and Milestone systems is to investigate crimes, aid in the prosecution of criminals, and monitor subjects inside SPD facilities. Additionally, these systems are used to monitor internal SPD operations and document police activities.

DRAFT

4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

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. Logs of system activity are kept for both automatic system functions and user actions which provide an audit trail to safeguard against potential unauthorized access to stored information.

The entire system is located on the SPD network which is protected by industry standard firewalls. The Seattle IT Department performs routine monitoring of the SPD network.

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.

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

ITD client services interaction with SPD systems is governed according to the terms of the 2018 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."

DRAFT

5.0 Data Storage, Retention and Deletion

5.1 How will data be securely stored?

Genetec (interview rooms): The original recordings are stored on a proprietary Genetec server that is located in a secure server room located in SPD HQ. The long-term storage copy produced by the detective is retained at the SPD Evidence Section following standard evidence retention rules.

Milestone (BAC rooms and precinct holding cells): Individual local servers are securely located all SPD precincts.

Per the CJIS Security Policy, each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunication lines; personnel security to include background screening requirements; technical security to protect against unauthorized use; data security to include III use, dissemination, and logging; and security of criminal history 08/16/2018 CJISD-ITS-DOC-08140-5.7 D-3 records. Additionally, each CSO (CJIS Systems Officer, or department command personnel) must ensure that all agencies establish an information security structure that provides for an ISO and complies with the CJIS Security Policy.

Both the Genetec and Milestone systems retain recordings for 90 days before they are automatically and systematically deleted from the server.

5.2 How will the owner allow for departmental and other entities, to audit for compliance with legal deletion requirements?

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.

5.3 What measures will be used to destroy improperly collected data?

Both the Genetec and Milestone systems retain recordings for 90 days before they are automatically and systematically deleted from the server.

SPD policy contains multiple provisions to avoid improperly collecting data. SPD Policy 7.010 governs the submission of evidence and requires that all collected evidence be documented in an incident report. SPD Policy 7.090 specifically governs the collection and submission of photographic evidence. Evidence is submitted to the Evidence Unit and associated with a specific GO Number and investigation. And, SPD Policy 7.110 governs the collection and submission of audio recorded statements. It requires that officers state their name, the Department name, the General Offense number, date and time of recording, the name of the interviewee, and all persons present at the beginning of the recording.
Additionally, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

DRAFT

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. SPD Policy 5.001 also ensures that communication on the systems subject to collection on this system is official in nature.

Per the CJIS Security Policy:
5.8.3 Digital Media Sanitization and Disposal The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

5.8.4 Disposal of Physical Media Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

DRAFT

5.4 which specific departmental unit or individual is responsible for ensuring compliance with data retention requirements?

Unit managers are responsible for ensuring compliance with data retention requirements within SPD. 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.

6.0 Data Sharing and Accuracy

6.1 Which entity or entities inside and external to the City will be data sharing partners?

No person, outside of SPD and Seattle IT, has direct access to the application or the data.

Data obtained from the system may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law.

Data may be shared with outside entities in connection with criminal prosecutions:

- Seattle City Attorney's Office
- King County Prosecuting Attorney's Office
- King County Department of Public Defense
- Private Defense Attorneys
- Seattle Municipal Court
- King County Superior Court
- Similar entities where prosecution is in Federal or other State jurisdictions

Data may be made available to requesters pursuant to the Washington Public Records Act, Chapter 42.56 RCW ("PRA"). SPD will apply applicable exemptions to the data before disclosing to a requester. Individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.

SPD shares data with authorized researchers pursuant to properly execute research and confidentiality agreements as provide by SPD Policy 12.055. This sharing may include discrete pieces of data related to specific investigative files collected by the system.

6.2 Why is data sharing necessary?

The sharing of recorded audio-video of police interviews of victims, witnesses, and crime suspects is often needed to aid in the prosecution of cases. Recordings may be shared only within the context of the situations outlined in 6.1.

6.3 Are there any restrictions on non-City data use?

Yes ☒ No ☐

6.3.1 if you answered yes, provide a copy of the department's procedures and policies for ensuring compliance with these restrictions.

Law enforcement agencies receiving criminal history information are subject to the requirements of 28 CFR Part 20, regulating criminal justice information systems. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260 (auditing and dissemination of criminal history record information systems), and RCW Chapter 10.97 (Washington State Criminal Records Privacy Act).

Once disclosed in response to PRA request, there are no restrictions on non-City data use; however, applicable exemptions will be applied prior to disclosure to any requestor who is not authorized to receive exempt content.

6.4 how does the project/technology review and approve information sharing agreements, memorandums of understanding, new uses of the information, new access to the system by organizations within City of Seattle and outside agencies?

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.

6.5 explain how the project/technology checks the accuracy of the information collected. If accuracy is not checked, please explain why.

The audio and video captured by these systems are real-time recordings of the interviews and activities that take place in view of the cameras permanently mounted in the interview and BAC rooms and within precinct holding cells.

6.6 describe any procedures that allow individuals to access their information and correct inaccurate or erroneous information.

Individuals may request records pursuant to the PRA, and individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.

DRAFT

7.0 Legal Obligations, Risks and Compliance

7.1 What specific legal authorities and/or agreements permit and define the collection of information by the project/technology?

Though the state of Washington is not one of the 26 states that requires the recording of custodial interrogations, many law enforcement agencies and criminal justice system watchdogs, such as the Innocence Project, highly recommend the practice.

Consent is required before these technologies may be used. **RCW 9.73.030 Intercepting, recording or divulging private communication – Consent required – Exceptions.** Also known as "All party consent". Standard procedure dictates that interview subjects are always advised of the presence of the recording or asked for their permission to record.

Additionally, **RCW 9.73.090 Certain emergency response personnel exempted from RCW 9.73.030 through 9.73.080—Standards—Court authorizations—Admissibility** states:

(b) Video and/or sound recordings may be made of arrested persons by police officers responsible for making arrests or holding persons in custody before their first appearance in court. Such video and/or sound recordings shall conform strictly to the following:

(i) The arrested person shall be informed that such recording is being made and the statement so informing him or her shall be included in the recording;

(ii) The recording shall commence with an indication of the time of the beginning thereof and terminate with an indication of the time thereof;

(iii) At the commencement of the recording the arrested person shall be fully informed of his or her constitutional rights, and such statements informing him or her shall be included in the recording;

(iv) The recordings shall only be used for valid police or court activities;

7.2 Describe what privacy training is provided to users either generally or specifically relevant to the project/technology.

SPD Policy 12.050 mandates that all employees receive Security Awareness Training (Level 2), and all employees also receive City Privacy Training. All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), many of which contain specific privacy requirements. 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 Given the specific data elements collected, describe 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.

DRAFT

The nature of the Department's mission will inevitably lead it to collect and maintain information many may believe to be private and potentially embarrassing. Minimizing privacy risks revolve around disclosure of personally identifiable information.

SMC 14.12 and SPD Policy 6.060 direct all SPD personnel that "any documentation of information concerning a person's sexual preferences or practices, or their political or religious activities must be for a relevant reason and serve a legitimate law enforcement purpose."

Further, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

7.4 Is there any aspect of the project/technology that might cause concern by giving the appearance to the public of privacy intrusion or misuse of personal information?

The privacy risks outlined in 7.3 above are mitigated by legal requirements and auditing processes (i.e., maintenance of all requests, copies of consent forms/statements and warrants) that allow for any auditor, including the Office of Inspector General and the federal monitor, to inspect the collection of recorded interactions between SPD and the public.

The greatest privacy risk is the unauthorized release of interview, BAC room, and holding cell video and audio recording that may contain information deemed private or offensive. To mitigate this risk, the technologies fall under the current SPD policies around dissemination of Department data and information reflected in 6.1.

DRAFT

8.0 Monitoring and Enforcement

8.1 describe how the project/technology maintains a record of any disclosures outside of the department.

Per SPD Policy 12.080, the Crime Records Unit is responsible to receive and record all requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies." Any subpoenas and requests for public disclosure are logged by SPD's Legal Unit. Any action taken, and data released subsequently in response to subpoenas is then tracked through a log maintained by the Legal Unit. Public disclosure requests are tracked through the City's GovQA Public Records Response System, and responses to Public Disclosure Requests, including responsive records provided to a requestor, are retained by SPD for two years after the request is completed.

8.2 what auditing measures are in place to safeguard the information, and policies that pertain to them, as well as who has access to the audit data? Explain whether the project/technology conducts self-audits, third party audits or reviews.

SPD's Audit, Policy and Research Section is authorized to conduct audits of all investigative data collection software and systems, including DEMS. In addition, the Office of Inspector General and the federal monitor can conduct audits of the software, and its use, at any time. Audit data is available to the public via Public Records Request.

Financial Information

Purpose

This section provides a description of the fiscal impact of the surveillance technology, as required by the surveillance ordinance.

1.0 Fiscal Impact

Provide a description of the fiscal impact of the project/technology by answering the questions below.

1.1 Current or potential sources of funding: initial acquisition costs.

Current ☒ potential ☐

DRAFT

Date of initial acquisition	Date of go live	Direct initial acquisition cost	Professional services for acquisition	Other acquisition costs	Initial acquisition funding source
(Genetec)6/28/2016	Aug 2016	$60,603.16			P7710
(Milestone) 6/14/2016	Aug 2016	$19,520.79			P8830

Notes:

1.2 Current or potential sources of funding: on-going operating costs, including maintenance, licensing, personnel, legal/compliance use auditing, data retention and security costs.

Current ☒ potential ☐

Annual maintenance and licensing	Legal/compliance, audit, data retention and other security costs	Department overhead	IT overhead	Annual funding source
(Genetec) $660.06				P7715
(Milestone) $3,698.91				P3348

Notes:

1.3 Cost savings potential through use of the technology

These are not quantified; however, potential cost savings may result from better evidence for crime prosecution and mitigating liability for complaints of misconduct of SPD personnel in BAC rooms and precinct holding cells.

1.4 Current or potential sources of funding including subsidies or free products offered by vendors or governmental entities

N/A

DRAFT

Expertise and References

Purpose

The following information is provided to ensure that Council has a group of experts to reference while reviewing the completed surveillance impact report ("SIR"). Any individuals or agencies referenced must be made aware ahead of publication that their information has been included. All materials must be available for Council to access or review, without requiring additional purchase or contract.

1.0 Other Government References

1.1 Please list any other government bodies that have implemented this technology and can speak to the implementation of this technology.

Agency, municipality, etc.	Primary contact	Description of current use

2.0 Academics, Consultants, and Other Experts

2.1 Please list any experts in the technology under consideration, or in the technical completion of the service or function the technology is responsible for.

Agency, municipality, etc.	Primary contact	Description of current use

3.0 White Papers or Other Documents

3.1 Please list any authoritative publication, report or guide that is relevant to the use of this technology or this type of technology.

DRAFT

Title	Publication	Link
"Preventing police torture and other forms of ill-treatment – reflections on good practices and emerging approaches"	28th General Report of the European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (CPT), published in 2019	https://rm.coe.int/1680942329
"Electronic Recording of Custodial Interrogations"	TheJusticeProject.org	https://web.williams.edu/Psychology/Faculty/Kassin/files/Justice%20Project(07).pdf

DRAFT

Racial Equity Toolkit ("RET") and Engagement for Public Comment Worksheet

Purpose

Departments submitting a SIR are required to complete an adapted version of the Racial Equity Toolkit ("RET") in order to:

- Provide a framework for the mindful completion of the SIR in a way that is sensitive to the historic exclusion of vulnerable and historically underrepresented communities. Particularly, to inform the public engagement efforts departments will complete as part of the surveillance impact report.
- Highlight and mitigate any impacts on racial equity from the adoption and the use of the technology.
- Highlight and mitigate any disparate impacts on individuals or vulnerable communities.
- Fulfill the public engagement requirements of the surveillance impact report.

Adaption of the RET for Surveillance Impact Reports

The RET was adapted for the specific use by the Seattle Information Technology departments' ("Seattle IT") privacy team, the Office of Civil Rights ("OCR"), and change team members from Seattle IT, Seattle City Light, Seattle Fire Department, Seattle Police Department, and Seattle Department of Transportation.

Racial Equity Toolkit Overview

The vision of the Seattle Race and Social Justice Initiative is to eliminate racial inequity in the community. To do this requires ending individual racism, institutional racism and structural racism. The racial equity toolkit lays out a process and a set of questions to guide the development, implementation and evaluation of policies, initiatives, programs, and budget issues to address the impacts on racial equity.

1.0 Set Outcomes

1.1. Seattle City Council has defined the following inclusion criteria in the surveillance ordinance, and they serve as important touchstones for the risks departments are being asked to resolve and/or mitigate. Which of the following inclusion criteria apply to this technology?

☐ The technology disparately impacts disadvantaged groups.

☐ There is a high likelihood that personally identifiable information will be shared with non-City entities that will use the data for a purpose other than providing the City with a contractually agreed-upon service.

☒ The technology collects data that is personally identifiable even if obscured, de-identified, or anonymized after collection.

DRAFT

☐ The technology raises reasonable concerns about impacts to civil liberty, freedom of speech or association, racial equity, or social justice.

1.2 What are the potential impacts on civil liberties through the implementation of this technology? How is the department mitigating these risks?

Inherent with any video or audio recording obtained and stored by SPD, personally identifiable and potentially sensitive personal information is collected about community members, including information about 3rd parties not present during the recordings.

1.3 What are the risks for racial or ethnicity-based bias through each use or deployment of this technology? How is the department mitigating these risks?

The mission of the Seattle Police Department is to prevent crime, enforce the law, and support quality public safety by delivering respectful, professional and dependable police services. A potential civil liberties concern is that the SPD would over-surveil vulnerable or historically targeted communities. SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures. The video systems described in this report are permanently installed inside SPD facilities and record individuals who are interacting with SPD personnel or are being held in precinct holding cells.

1.4 Where in the City is the technology used or deployed?

☒ all Seattle neighborhoods

☐ Ballard	☐ Southeast
☐ North	☐ Delridge
☐ Northeast	☐ Greater Duwamish
☐ Central	☐ East district
☐ Lake union	☐ King county (outside Seattle)
☐ Southwest	☐ Outside King County.

If possible, please include any maps or visualizations of historical deployments / use.

1.4.1 What are the racial demographics of those living in this area or impacted by these issues?

DRAFT

City of Seattle demographics: White - 69.5%; Black or African American - 7.9%; Amer. Indian & Alaska Native - 0.8%; Asian - 13.8%; Native Hawaiian & Pacific Islander - 0.4; Other race - 2.4%; Two or more races - 5.1%; Hispanic or Latino ethnicity (of any race): 6.6%; Persons of color: 33.7%.

King County demographics: White – 70.1%; Black or African American – 6.7%; American Indian & Alaskan Native – 1.1%; Asian, Native Hawaiian, Pacific Islander – 17.2%; Hispanic or Latino (of any race) – 9.4%

1.4.2 How are decisions made where the technology is used or deployed? How does the Department work to ensure diverse neighborhoods are not specifically targeted?

The Genetec system (Interview rooms) is located at SPD Headquarters. The Milestone system (BAC rooms and precinct holding cells) is located at all SPD precincts throughout the City of Seattle.

1.5 How do decisions around data sharing have the potential for disparate impact on historically targeted communities? What is the department doing to mitigate those risks?

The Aspen Institute on Community Change defines structural racism as "…public policies, institutional practices, cultural representations and other norms [which] work in various, often reinforcing ways to perpetuate racial group inequity." Data sharing has the potential to be a contributing factor to structural racism and thus creating a disparate impact on historically targeted communities. In an effort to mitigate this possibility, SPD has established policies regarding the dissemination of data in connection with criminal prosecutions, Washington Public Records Act (Chapter 42.56 RCW), and other authorized researchers.

Further, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

Video and audio collected by the Genetec and Milestone systems, is shared only with outside entities in connection with criminal prosecutions or in compliance with public records requests pursuant to the Washington Public Records Act, Chapter 42.56 RCW ("PRA"). SPD will apply applicable exemptions to the data before disclosing to a requester.

1.6 How do decisions around data storage and retention have the potential for disparate impact on historically targeted communities? What is the department doing to mitigate those risks?

Like decisions around data sharing, data storage and retention have similar potential for disparate impact on historically targeted communities. SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

DRAFT

1.7 What are potential unintended consequences (both negative and positive potential impact)? What proactive steps can you can / have you taken to ensure these consequences do not occur.

The most important unintended possible consequence related to the continued utilization of the Genetec and Milestone camera systems by SPD is the potential that members of the public will be recorded without their consent. SPD Policy 7.110 – Recorded Statements forbids SPD personnel from making such recordings without consent, except in specific exigent circumstances without proper warrant. Additionally, SPD policies, including SPD Policy 6.060 - Collection of Information for Law Enforcement Purposes also defines the way information will be gathered by SPD and states, "information will be gathered and recorded in a manner that does not unreasonably infringe upon: individual rights, liberties, and freedoms guaranteed by the Constitution of the United States and the State of Washington, including freedom of speech, press, association, and assembly; liberty of conscience; the exercise of religion…"

2.0 Public Outreach

2.1 Organizations who received a personal invitation to participate.

Please include a list of all organizations specifically invited to provide feedback on this technology.

2.1 Scheduled public meeting(s).

Meeting notes, sign-in sheets, all comments received, and questions from the public will be included in Appendix A-C. Comment analysis will be summarized in section 3.0 Public Comment Analysis.

Meeting 1

Date	
Time	
Capacity	

2.2 Scheduled focus Group Meeting(s)

Meeting 1

DRAFT

Community	
Date	

3.0 Public Comment Analysis

This section will be completed after the public comment period has been completed on [DATE].

3.1 Demographics of the public who submitted comments.

Dashboard of respondent demographics.

3.2 Survey Monkey public comments received.

Dashboard of respondent demographics.

3.3 Focus group public comments received.

Dashboard of respondent demographics.

3.4 Digital town hall public comments received.

Dashboard of respondent demographics.

3.5 General surveillance comments received during this public comment period.

Dashboard of respondent demographics.

4.0 Response to Public Comments

This section will be completed after the public comment period has been completed on [DATE].

4.1 How will you address the concerns that have been identified by the public?

What program, policy and partnership strategies will you implement? What strategies address immediate impacts? Long-term impacts? What strategies address root causes of inequity listed above? How will you partner with stakeholders for long-term positive change?

5.0 Equity Annual Reporting

5.1 What metrics for this technology be reported to the CTO for the annual equity assessments? Departments will be responsible for sharing their own evaluations with department leadership, change team leads, and community leaders identified in the public outreach plan.

Respond here.

DRAFT

DRAFT

Privacy and Civil Liberties Assessment

Purpose

This section shall be completed after public engagement has concluded and the department has completed the racial equity toolkit section above. The privacy and civil liberties assessment is completed by the community surveillance working group ("working group"), per the surveillance ordinance which states that the working group shall:

"Provide to the executive and the City Council a privacy and civil liberties impact assessment for each SIR that must be included with any departmental request for surveillance technology acquisition or in-use approval. The impact assessment shall include a description of the potential impact of the surveillance technology on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities. The CTO shall share with the working group a copy of the SIR that shall also be posted during the period of public engagement. At the conclusion of the public engagement period, the CTO shall share the final proposed SIR with the working group at least six weeks prior to submittal of the SIR to Council for approval. The working group shall provide its impact assessment in writing to the executive and the City Council for inclusion in the SIR within six weeks of receiving the final proposed SIR. If the working group does not provide the impact assessment before such time, the working group must ask for a two-week extension of time to City Council in writing. If the working group fails to submit an impact statement within eight weeks of receiving the SIR, the department and City Council may proceed with ordinance approval without the impact statement."

Working Group Privacy and Civil Liberties Assessment

Respond here.

DRAFT

Appendix A: Glossary

Accountable: (taken from the racial equity toolkit.) Responsive to the needs and concerns of those most impacted by the issues you are working on, particularly to communities of color and those historically underrepresented in the civic process.

Community outcomes: (taken from the racial equity toolkit.) The specific result you are seeking to achieve that advances racial equity.

Contracting equity: (taken from the racial equity toolkit.) Efforts to achieve equitable racial outcomes in the way the City spends resources, including goods and services, consultants and contracting.

DON: "department of neighborhoods."

Immigrant and refugee access to services: (taken from the racial equity toolkit.) Government services and resources are easily available and understandable to all Seattle residents, including non-native English speakers. Full and active participation of immigrant and refugee communities exists in Seattle's civic, economic and cultural life.

Inclusive outreach and public engagement: (taken from the racial equity toolkit.) Processes inclusive of people of diverse races, cultures, gender identities, sexual orientations and socio-economic status. Access to information, resources and civic processes so community members can effectively engage in the design and delivery of public services.

Individual racism: (taken from the racial equity toolkit.) Pre-judgment, bias, stereotypes about an individual or group based on race. The impacts of racism on individuals including white people internalizing privilege, and people of color internalizing oppression.

Institutional racism: (taken from the racial equity toolkit.) Organizational programs, policies or procedures that work to the benefit of white people and to the detriment of people of color, usually unintentionally or inadvertently.

OCR: "Office of Civil Rights."

Opportunity areas: (taken from the racial equity toolkit.) One of seven issue areas the City of Seattle is working on in partnership with the community to eliminate racial disparities and create racial equity. They include: education, health, community development, criminal justice, jobs, housing, and the environment.

Racial equity: (taken from the racial equity toolkit.) When social, economic and political opportunities are not predicted based upon a person's race.

DRAFT

Racial inequity: (taken from the racial equity toolkit.) When a person's race can predict their social, economic, and political opportunities and outcomes.

RET: "racial equity toolkit"

Seattle neighborhoods: (taken from the racial equity toolkit neighborhood.) Boundaries defined for the purpose of understanding geographic areas in Seattle.

Stakeholders: (taken from the racial equity toolkit.) Those impacted by proposed policy, program, or budget issue who have potential concerns or issue expertise. Examples might include: specific racial/ethnic groups, other institutions like Seattle housing authority, schools, community-based organizations, change teams, City employees, unions, etc.

Structural racism: (taken from the racial equity toolkit.) The interplay of policies, practices and programs of multiple institutions which leads to adverse outcomes and conditions for communities of color compared to white communities that occurs within the context of racialized historical and cultural conditions.

Surveillance ordinance: Seattle City Council passed ordinance 125376, also referred to as the "surveillance ordinance."

SIR: "surveillance impact report", a document which captures the fulfillment of the Council-defined surveillance technology review process, as required by ordinance 125376.

Workforce equity: (taken from the racial equity toolkit.) Ensure the City's workforce diversity reflects the diversity of Seattle.

DRAFT

Appendix B: Meeting Notice(s)

Appendix C: Meeting sign-in sheet(s)

Appendix D: All Comments Received from Members of the Public

Appendix E: Department Responses to Public Inquiries

Appendix F: Letters from Organizations or Commissions

Appendix G: CTO Notification of Surveillance Technology

DRAFT