City of Seattle

2019 Surveillance Impact Report

911 Logging Recorder

Seattle Police Department

Table of Contents

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. 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".
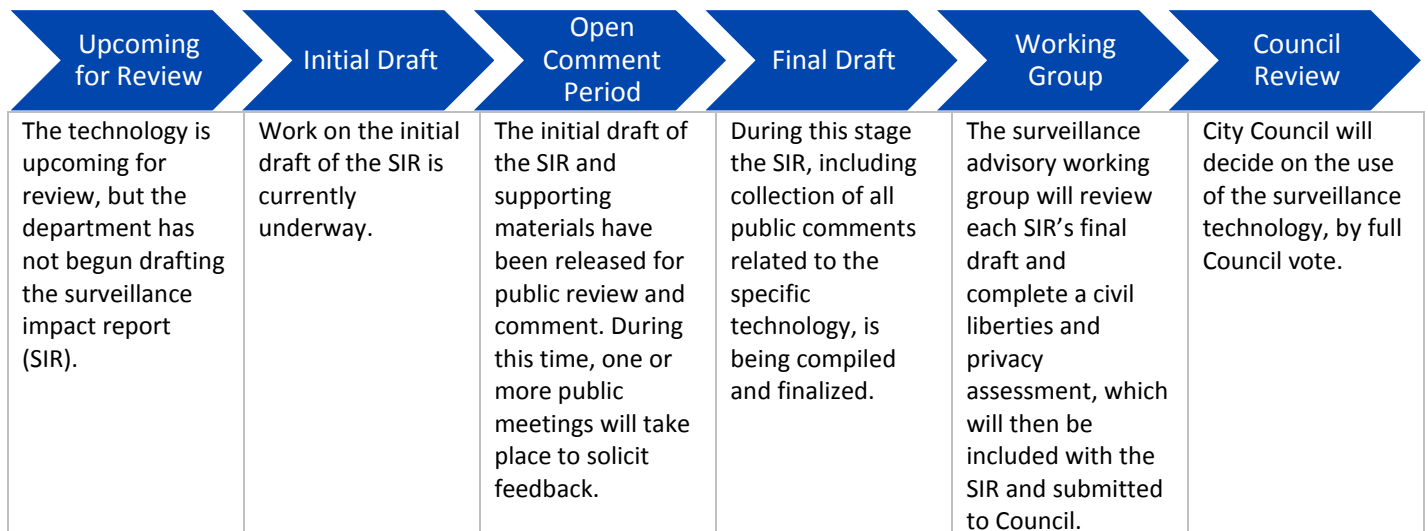
How this Document is Completed

This document is completed by the requesting department staff, support and coordinated by the Seattle information technology department ("Seattle it"). As Seattle it and department staff complete the document, they should keep the following in mind.

1. Responses to questions should be in the text or check boxes only; all other information (questions, descriptions, etc.) Should **not** be edited by the department staff completing this document.

2. All content in this report will be available externally to the public. With this in mind, avoid using acronyms, slang, or other terms which may not be well-known to external audiences. Additionally, responses should be written using principally non-technical language to ensure they are accessible to audiences unfamiliar with the topic.

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.

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.

> The NICE 9-1-1 Logging Recorder audio-records all telephone calls to SPD's 9-1-1 communications center and all radio traffic between dispatchers and patrol officers.

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

> This application automatically records telephone calls received by the 9-1-1 communications center. The content and nature of those phone calls may include highly sensitive information such as the caller's name, phone number, address from which they are calling, medical conditions, detailed information about suspects, witnesses, or victims of a crime or other emergency events, and potentially other personally identifiable information. Callers may report personally-identifying information about third parties without providing notice to those individuals. While most of this information is consciously volunteered by callers, some of the information may be stored for future reference in emergency situations, for quality assurance purposes, or as evidence in a criminal investigation.

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.

This technology audio-records 9-1-1 and non-emergency telephone calls and police radio traffic for evidentiary and public disclosure purposes.   Audio recordings are routinely used in criminal prosecutions and are routinely used within the 9-1-1 Center for training and quality control purposes.

Recordings of 9-1-1 calls and radio traffic are routinely provided to detective units to assist in criminal investigations. In addition, SPD provides approximately 5000 recordings to the Seattle Law Department each year to support legal proceedings Recordings are also used as a quality assurance measure to review calls to ensure that call takers and dispatchers are following SPD policies and procedures and to ensure SPD practices meet or exceed industry standards.

2.2 Provide any data or research demonstrating anticipated benefits.

The National Emergency Number Association's E9-1-1 PSAP (Public Safety Answering Point) Equipment Standards, a standard that defines PSAP equipment requirements for providers of 9-1-1 services, states, "as a minimum, each 9-1-1 call must be recorded." (https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/nena-sta-027.3-2018_20180702.pdf)

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. Audio recordings of 9-1-1 calls and police radio traffic can provide critical evidence to officers and detectives who investigate crimes and the prosecutors who prosecute offenders. These recordings also provide transparency and accountability for SPD, as they record in real time the interactions between 9-1-1 call takers and callers, and the radio traffic between 9-1-1 dispatchers and police officers. The NICE system also supports the 9-1-1 center's mission of quickly determining the nature of the call and getting the caller the assistance they need as quickly as possible with high quality, consistent and professional services.

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

SPD's authorized users of the NICE 9-1-1 Logging Recorder include police communications analysts who routinely capture audio recordings germane to police investigations and forward those recordings to detective units, outside legal entities such as the City Attorney's Office, the King County Prosecutor's Office and defense attorneys. Police Communications Supervisors and Analysts routinely listen to audio recordings for Quality Assurance purposes. The 9-1-1 Recordings Office is overseen by the 9-1-1 Administrative Manager.

Additionally, Seattle IT provides client services and operational support for IT technologies and applications. In supporting SPD systems, operational and application services deploy and service SPD technology systems. Details about the IT department are found in the appendix of this SIR.

All authorized users of the NICE 9-1-1 Logging Recorder are Criminal Justice Information Services (CJIS) certified and maintain Washington State ACCESS (A Central Computerized Enforcement Service System) certification. More information on CJIS compliance may be found at the CJIS Security Policy website. Additional information about ACCESS may be found on the Washington State Patrol's website.

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.

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.

The technology is used in two distinct ways. Primarily it automatically records all calls into the 9-1-1 system, police non-emergency phone line, and police radio traffic. Secondarily, it is used to retrieve recordings by authorized personnel.

Authorized SPD users may access the recordings by logging into the NICE 9-1-1 Logging Recorder utilizing a unique user name and password. Access for personnel into the system is predicated on state and federal law governing access to criminal justice information systems. This includes thorough background investigations for each user, appropriate access and permissions dependent on the personnel role, and an audit of access and transaction logs within the system.

For information regarding CJIS security and compliance policies, see Appendices K and M of this SIR.

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

The technology is used to record all telephone calls between the public and the 9-1-1 Center, and police radio traffic. This is triggered when a community member contacts the department by calling 9-1-1 or the departments non-emergency numbers, including all outbound calls placed by 9-1-1 call takers and dispatchers and all radio traffic between dispatchers and police personnel including police officers, parking enforcement officers, and police detectives utilizing the police radio system.

Requests for audio recordings are initiated by detective units investigating a crime, legal counsel, and other outside entities. Recordings may also be initiated by the public using the Public Disclosure Process.

In addition, RCW 9.73.090 permits police, fire, emergency medical service, emergency communication center, and poison control center personnel to record incoming telephone calls to police and fire stations, licensed emergency medical service providers, emergency communication centers, and poison centers.

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.

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. Supervisors and commanding officers are responsible for ensuring compliance with SPD policies.

Data is securely input and used on SPD's password-protected network with access limited to authorized detectives and identified supervisory personnel.

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 Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures. 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 Communications Section Policy 3.005 – Employee Conduct.

ITD client services interaction with SPD systems is governed by the terms of the 2018 Management Control Agreement (MCA)t 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 there fore required to support, enable, enforce and comply with SPD policy requirements, including the FBIs Criminal Justice Information Services, (CJIS) Security Policy."

The MCA document may be found in Appendix K. Per the CJIS security policy, records of individual basic security awareness training and specific information system security training shall be documented, kept current, and maintained. Details of the compliance program in Appendix M.

4.0 Data Collection and Use

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.

No information is collected from a source other than individual who calls 9-1-1 or from the officers and dispatchers.

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

The 9-1-1 audio recordings do not verify whether the information that was collected is accurate. They record, in real time, conversations between 9-1-1 callers and call takers. Only calls to the 9-1-1 system and specific designated phone lines are logged and recorded. Calls to other SPD phone lines are not recorded by this system. The telephone lines which SPD records are 9-1-1, the department's published non-emergency number, and the department's non-published 10-digit direct line to SPD dispatch. These telephone lines are used by the public to report crimes to the department and/or request police services. This system does not record conversations on any desk phone assigned to specific individuals within the department. Audio recordings that have not been requested within 90 days of their capture are deleted. Recordings requested for law enforcement and public disclosure are downloaded and maintained for the retention period related to the incident type.

Use of the technology other than the recording of calls to and from 9-1-1, police radio traffic, and retrieval of those recordings for law enforcement or public disclosure purposes is out of policy and subject to SPD disciplinary action.

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?

The NICE 9-1-1 Logging Recorder is automatically used to record all calls into the 9-1-1 system, police non-emergency phone line, and police radio traffic. Police communications analysts also routinely use the NICE 9-1-1 Logging Recorder to capture audio recordings germane to police investigations and forward those recordings to detective units, outside legal entities such as the Seattle City Attorneys' Office, the King County Prosecutors Office, and defense attorneys. Police Communications Supervisors and Analysts routinely listen to audio recordings for Quality Assurance purposes. The 9-1-1 Recordings Office is overseen by the 9-1-1 Administrative Manager.

4.4 How often will the technology be in operation?

The 9-1-1 audio recordings are automatic and are ongoing on a 24/7 basis.

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

The NICE 9-1-1 Logging Recorder is a permanent installation.

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?

Per Washington State law, ([RWC 9.73.030](#)) communications of an emergency nature are not included in the requirement to obtaining consent to record. Audio recordings are made available to the public only via the Public Disclosure Request process. Audio recordings that are not requested within 90 days of their capture are deleted.

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

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.

Data is securely input and used on SPD's password-protected network with access limited to authorized detectives and identified supervisory personnel.

Per the CJIS security Policy:

"The agency shall configure the application, service, or information system to provide only essential capabilities and shall specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services."

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.

Incidental data access may be necessary through delivery of technology client services. All ITD employees are required to comply with appropriate regulatory requirements regarding security and background review. ITD CJIS Policy, the remote access policy, and information on ITD client services support roles related to this technology can be found in Appendices K and M.

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."

The MCA document may also be found in Appendix K.

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

This application is used by Seattle Police staff and occasionally Seattle Fire Department staff when they are in place at their backup 9-1-1 positions located at West Police Precinct. The software vendor NICE is given escorted access as needed (on site or via remote Web Ex connection) to help triage problems, configure system settings, and resolve technical issues. There is an annual maintenance contract with NICE for this system support. This system is not accessible by any outside entity without making a specific request to the Seattle Police Department through official means.

As mentioned, Seattle IT Department personnel have administrative access to the system for support services. As such, incidental data access may occur through delivery of technology client services.

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

Verified users access the system to capture and disseminate audio recordings based on the requests received from detective units, outside legal entities, and the public.

Incidental data access may occur through delivery of technology client services. All ITD employees are required to comply with appropriate regulatory requirements regarding security and background review.

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."

Incidental access to the data may also occur by way of ITD services. The CJIS remote access policy is applicable here and can be found in the appendices of this document.

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.

Data is securely input and used on SPD's password-protected network with access limited to authorized detectives and identified supervisory personnel.

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."

This MCA document may be found in Appendix K.

Additionally, per the CJIS Security Policy, the following safeguards are in place:

- The agency shall establish identifier and authenticator processes.

- Two-factor authentication employs the use of two of the following three factors of authentication: something you know (e.g. 08/16/2018 CJISD-ITS-DOC-08140-5.7 37 password), something you have (e.g. hard token), something you are (e.g. biometric). The two authentication factors shall be unique (i.e. password/token or biometric/password but not password/password or token/token).

- Unsuccessful login attempts - the system shall enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI). The system shall automatically lock the account/node for a 10 minute time period unless released by an administrator.

- When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via encryption. When encryption is employed, the cryptographic module used shall be FIPS 140-2 certified and use a symmetric cipher key strength of at least 128 bit strength to protect CJI.

- When CJI is at rest (i.e. stored digitally) outside the boundary of the physically secure location, the data shall be protected via encryption. When encryption is employed, agencies shall either encrypt CJI in accordance with the standard in Section 5.10.1.2.1 above, or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256 bit strength.

- Intrusion Detection Tools/Techniques such as monitor inbound and outbound communications for unusual or unauthorized activities, send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort, employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.

- Audit - Each agency shall be responsible for complying with all audit requirements for use of CJIS Systems. Each CSO is responsible for completing a triennial audit of all agencies with access to CJIS Systems through the CSO's lines.

- The agency's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The agency shall periodically review and update the list of agency-defined auditable events. In the event an agency does not use an automated system, manual recording of activities shall still take place.

- A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage.

Publicly accessible computers shall not be used to access, process, store or transmit CJI.

5.0 Data Storage, Retention and Deletion

5.1 How will data be securely stored?

The data is stored in the NICE system, much of the NICE system is physically housed at the SPD 9-1-1 center, with some of the servers hosted virtually on SPD network in SPD section of the city data center. Data collect is located on the server's storage in the above locations. Extracted data is stored on file shares for SPD and City Law (these reside SPD Network Storage or Law storage system managed by Seattle ITD). Extracted data is electronically sent to Law, Discovery or as redacted material in response to PDR (posted to the City PDR system, GOVQA).

Per the CJIS Security Policy found in Appendix M:

Security - 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 must ensure that all agencies establish an information security structure that provides for an ISO and complies with the CJIS Security Policy.

Network Diagrams - Network diagrams, i.e. topological drawings, are an essential part of solid network security. Through graphical illustration, a comprehensive network diagram provides the "big picture" – enabling network managers to quickly ascertain the interconnecting nodes of a network for a multitude of purposes, including troubleshooting and optimization. Network diagrams are integral to demonstrating the manner in which each agency ensures criminal justice data is afforded appropriate technical security protections and is protected during transit and at rest.

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.

The 2017 Technical Security Audit for CJIS Compliance for SPD can be found in Appendix K.

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

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 a GO 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.

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.

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.

The CJIS security policy in Appendix M of this SIR includes applicable data retention requirements associated with the CAD system. The MCA between SPD and ITD is the inter-departmental agreement that ensures compliance with the CJIS Security Policy, and can be found in Appendices K and M.

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.

As Seattle IT supports the NICE system on behalf of SPD, a Management Control Agreement exists between SPD and Seattle IT. The agreement outlines the specifications for compliance, and enforcement related to supporting the NICE system through inter-departmental partnership. The MCA can be found in the appendices of this SIR.

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.

Per SPD Policy 12.080, the Crime Records Unit is responsible for receiving, recording, and responding to requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies."

Discrete pieces of data collected by CAD may be shared with other law enforcement agencies in wanted bulletins, and in connection with law enforcement investigations jointly conducted with those agencies, or in response to requests from law enforcement agencies investigating criminal activity as governed by SPD Policy 12.050 and 12.110. All requests for data from Federal Immigration and Customs Enforcement (ICE) authorities are referred to the Mayor's Office Legal Counsel in accordance with the Mayoral Directive, dated February 6, 2018.

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?

Data sharing is not an automatic component of the 9-1-1 recording system. Instead, discrete 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 SPD business users typically inform IT support if the calls are not present or appear to be inaccurate in any manner. These phone lines are isolated for 9-1-1 traffic or Communications Center business needs only. The few lines that are business lines that come into the VIPER system are also being recorded. The recorded phone lines are identified and mapped to indicate which ones are 9-1-1 lines and which ones are not.

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.

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?

SPD's use of 9-1-1 audio recordings is governed by RCW 9.73, other legal requirements, and policies as outlined in 3.1, 3.2, 3.3, 4.2, 4.6, and 5.3 of this SIR.

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.

The CJIS training requirements can be found in the appendices of this document, as well as in question 3.3, above.

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.

Privacy risks may arise when information is collected about citizens, unrelated to a specific incident. These concerns are mitigated by policy and procedures. In addition, 9-1-1 audio recordings may capture highly sensitive and private incidents and 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." Additionally, officers must take care "when photographing demonstrations or other lawful political activities. If demonstrators are not acting unlawfully, police can't photograph them."

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.

Finally, see 5.3 for a detailed discussion about procedures related to noncompliance.

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 use and deployment of 9-1-1 audio recordings.

The largest privacy risk is the un-authorized release of 9-1-1 audio recordings that contained information deemed private or offensive in the RCW. To mitigate this risk, the technology falls under the current SPD policies around dissemination of Department data and information reflected in 6.1.

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.

All requests for data from Federal Immigration and Customs Enforcement (ICE) authorities are referred to the Mayor's Office Legal Counsel in accordance with the Mayoral Directive, dated February 6, 2018.

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. 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.

The latest CJIS technical security audit from 2017 can be found in Appendix K of this SIR.

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 ☐

Date of initial acquisition	Date of go live	Direct initial acquisition cost	Professional services for acquisition	Other acquisition costs	Initial acquisition funding source
12/20/2013	N/A	$116,729.23	$97,002.03	Tax: $20,304.47	General Fund, partially reimbursed by King County E 9-1-1

Notes:

N/A

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
$98,495				ITD for SPD

Notes:

"NICE GOLD System Support for the period 11/01/17 - 10/31/18. KC E911 Reimbursable up to 75%. Annual Renewal of NICE System Recorder at Comm Center NICE System Service Agreement (audio Recorder 9-1-1) for SFD"

1.3 Cost savings potential through use of the technology

These are not quantified; however, potential cost savings may result from enhancements to 9-1-1 center response through training and quality assurance practices.

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

KC E911 Reimbursable up to 75%.

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

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
None	None	None

2.0 Academics, Consultants, and Other Experts

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
None	None	None

3.0 White Papers or Other Documents

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

Title	Publication	Link
None	None	None

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.

Adaptation 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 ("RSJI") is to eliminate racial inequity in the community. To do this requires ending individual racism, institutional racism and structural racism. The RET 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.

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

Retroactive Technology Request By: SEATTLE POLICE DEPARTMENT

Racial Equity Toolkit ("RET") and Engagement for Public Comment Worksheet | Surveillance Impact Report | 911 LOGGING RECORDER |page 26

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

Some personally identifiable information (PII) gathered during emergency responses could be used to identify individuals, such as their name, home address or contact information.   Victims of criminal activity may also be identified during incident responses, whose identities should be protected in accordance with RCW 42.56.240 and RCW 70.02.

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?

Include a description of any issues that may arise such as algorithmic bias or the possibility for ethnic bias to emerge in people and/or system decision-making.

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. While race and ethnicity information of individuals may be recorded by the NICE 9-1-1 audio recording system, 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.

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

☒ all Seattle neighborhoods

☐ Ballard
☐ Belltown
☐ Beacon Hill
☐ Capitol Hill
☐ Central District
☐ Columbia City
☐ Delridge
☐ First Hill
☐ Georgetown
☐ Greenwood / Phinney
☐ International District
☐ Interbay
☐ North
☐ Northeast

☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☐ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake
☐ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County.

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

N/A

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

> The demographics for the City of Seattle: White - 69.5%; Black or African American - 7.9%; Amer. Indian & Alaska Native - 0.8%; Asian - 13.8%; Native Hawaiian & Other Pac. 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%.

1.4.2 How does the Department to ensure diverse neighborhoods, communities, or individuals are not specifically targeted through the use or deployment of this technology?

> The the NICE 9-1-1 Logging Recorderis used to record all calls placed to 9-1-1 and the police non-emergency numbers without regard to where the call originates from. There is no distinction in the levels of service this system provides to the various and diverse neighborhoods, communities, or individuals within the city.

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."[1] 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.
>
> No person outside of SPD has direct access to the application or the data recorded by the NICE 9-1-1 audio recording system. Data obtained by the system may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law.

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.

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 the NICE 9-1-1 Logging Recorder by SPD is the unintentional release of privacy data. All users of the the NICE 9-1-1 Logging Recorder must be CJIS certified and maintain Washington State ACCESS certification and existing SPD policies mitigate the risks of unintentional release of information.

Retroactive Technology Request By: SEATTLE POLICE DEPARTMENT

Racial Equity Toolkit ("RET") and Engagement for Public Comment Worksheet | Surveillance Impact Report | 911 LOGGING RECORDER |page 29

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.

1. ACLU of Washington	2. Ethiopian Community Center	3. Planned Parenthood Votes Northwest and Hawaii
4. ACRS (Asian Counselling and Referral Service)	5. Faith Action Network	6. PROVAIL
7. API Chaya	8. Filipino Advisory Council (SPD)	9. Real Change
10. API Coalition of King County	11. Friends of Little Saigon	12. SCIPDA
13. API Coalition of Pierce County	14. Full Life Care	15. Seattle Japanese American Citizens League (JACL)
16. CAIR	17. Garinagu HounGua	18. Seattle Neighborhood Group
19. CARE	20. Helping Link	21. Senior Center of West Seattle
22. Central International District Business Improvement District	23. Horn of Africa	24. Seniors in Action
25. Church Council of Greater Seattle	26. International ImCDA	27. Somali Family Safety Task Force
28. City of Seattle Community Police Commission (CPC)	29. John T. Williams Organizing Committee	30. South East Effective Development
31. City of Seattle Community Technology Advisory Board	32. Kin On Community Health Care	33. South Park Information and Resource Center SPIARC
34. City of Seattle Human Rights Commission	35. Korean Advisory Council (SPD)	36. STEMPaths Innovation Network
37. Coalition for Refugees from Burma	38. Latina/o Bar Association of Washington	39. University of Washington Women's Center
40. Community Passageways	41. Latino Civic Alliance	42. United Indians of All Tribes Foundation
43. Council of American Islamic Relations - Washington	44. LELO (Legacy of Equality, Leadership, and Organizing)	45. Urban League
46. East African Advisory Council (SPD)	47. Literacy Source	48. Wallingford Boys & Girls Club
49. East African Community Services	50. Millionair Club Charity	51. Washington Association of Criminal Defense Lawyers
52. Education for All	53. Native American Advisory Council (SPD)	54. Washington Hall
55. El Centro de la Raza	56. Northwest Immigrant Rights Project	57. West African Community Council
58. Entre Hermanos	59. OneAmerica	60. YouthCare
61. US Transportation expertise	62. Local 27	63. Local 2898
64. (SPD) Demographic Advisory Council	65. South Seattle Crime Prevention Coalition (SSCPC)	66. CWAC
67. NAAC		

2.1 Scheduled public meeting(s).

Meeting notes, sign-in sheets, all comments received, and questions from the public will be included in Appendix B, C, D, E, F, G, H and I. Comment analysis will be summarized in section 3.0 Public Comment Analysis.

Location	El Centro de la Raza: 1660 S Roberto Maestas Festival St. Seattle, WA 98144
Time	February 23, 2019; 11 a.m – 2 p.m.
Capacity	100+
Link to URL Invite	

2.2 Scheduled Focus Group Meeting(s)

Meeting 1

Community Engaged	
Date	

Meeting 2

Community Engaged	
Date	

Retroactive Technology Request By: SEATTLE POLICE DEPARTMENT

Racial Equity Toolkit ("RET") and Engagement for Public Comment Worksheet | Surveillance Impact Report | 911 LOGGING RECORDER |page 31

3.0 Public Comment Analysis

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

3.1 Summary of Response Volume

Dashboard of respondent demographics.

3.2 Question One: What concerns, if any, do you have about the use of this technology?

Dashboard of respondent demographics.

3.3 Question Two: What value, if any, do you see in the use of this technology?

Dashboard of respondent demographics.

3.4 Question Three: What would you want City leadership to consider when making a decision about the use of this technology?

Dashboard of respondent demographics.

3.5 Question Four: General response to the technology.

Dashboard of respondent demographics.

3.5 General Surveillance Comments

These are comments received that are not particular to any technology currently under review.

Dashboard of respondent demographics.

Retroactive Technology Request By: SEATTLE POLICE DEPARTMENT

Racial Equity Toolkit ("RET") and Engagement for Public Comment Worksheet | Surveillance Impact Report | 911 LOGGING RECORDER |page 32

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?

Retroactive Technology Request By: SEATTLE POLICE DEPARTMENT

Racial Equity Toolkit ("RET") and Engagement for Public Comment Worksheet | Surveillance Impact Report | 911 LOGGING RECORDER |page 33

5.0 Equity Annual Reporting

5.1 What metrics for this technology be reported to the CTO for the annual equity assessments?

Respond here.

Retroactive Technology Request By: SEATTLE POLICE DEPARTMENT

Racial Equity Toolkit ("RET") and Engagement for Public Comment Worksheet | Surveillance Impact Report | 911 LOGGING RECORDER |page 34

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.

Submitting Department Memo

Description

Provide the high-level description of the technology, including whether software or hardware, who uses it and where/when.

Purpose

State the reasons for the use cases for this technology; how it helps meet the departmental mission; benefits to personnel and the public; under what ordinance or law it is used/mandated or required; risks to mission or public if this technology were not available.

Benefits to the Public

Provide technology benefit information, including those that affect departmental personnel, members of the public and the City in general.

Privacy and Civil Liberties Considerations

Provide an overview of the privacy and civil liberties concerns that have been raised over the use or potential mis-use of the technology; include real and perceived concerns.

Summary

Provide summary of reasons for technology use; benefits; and privacy considerations and how we are incorporating those concerns into our operational plans.

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.

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.

Appendix B: Public Comment Analysis

Appendix C: Public Comment Demographics

Appendix D: Comment Analysis Methodology

Appendix E: Questions and Department Responses

Appendix F: Public Outreach Overview

Appendix G: Meeting Notice(s)

Appendix H: Meeting Sign-in Sheet(s)

Appendix I: All Comments Received from Members of the Public

Appendix J: Letters from Organizations or Commissions

Appendix K: Supporting Policy Documentation

Management Control Agreement

**Management Control Agreement Between
Seattle Police Department and
City of Seattle Information Technology Department**

The City of Seattle Police Department ("SPD"), also referred to as the Criminal Justice Agency, and the City of seattle Information Technology Department (''ITD") are departments of the municipal corporation of the City of Seattle.

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 FBl's Criminal Justice Information Services ("CJIS") Security Policy.

Pursuant to the CJIS Security Policy, it is agreed that with respect to the administration of computer systems, network infrastructure, devices, and services interfacing directly or indirectly with A Central Computerized Enforcement System ("ACCESS") for the exchange of criminal history/criminal justice information, the Criminal Justice Agency shall have the authority, via managed control, to set and enforce:

Priorities that guarantee the priority, integrity, and availability of service needed by the criminal justice community.

Requirements for the selection, authorization, supervision, and termination of physical and logical access to Criminal Justice Information ("CJI").

Policy governing operation of justice systems, data, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a communications network and related criminal justice systems to include but not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.

Restriction of unauthorized physical and logical access to or use of systems and equipment accessing CJI.

Compliance with all rules and regulations of the Criminal Justice Agency policies and CJIS Security Policy in the operation of, access to, or control over any CJI systems, data, or infrastructure.

The responsibility for management control of the criminal justice function remains solely with the Criminal Justice Agency. ITD will not enter into any agreements or allow any access to, possession of, or control over any SPD CJI systems, data, or infrastructure without explicit authorization from at least one SPD Authorized Party. SPD Authorized Parties must be SPD employees and include:
Chief of Police
Chief Operating Officer

This agreement covers the overall supervision of all Criminal Justice Agency systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, administration, and maintenance of any Criminal Justice Agency system to include NCIC Programs that may be subsequently designed and/or implemented within the Criminal Justice Agency.

Additional agreements, such as a Memorandum of Agreements, Service Level Agreements, and/or Continuity Plans, may be established and maintained to further delineate, define, and assign roles, responsibilities, and requirements of and agreements between SPD and ITD, and other City of Seattle Departments and/or agencies.

Tracye Cantrell   Date   Feb 2, 2018
Interim Chief Technology Officer
Seattle Information Technology Department

Carmen Best   Date   2-7-2018
Interim Chief of Police
Seattle Police Department

Reference: CJIS Security Policy, Version 5.5, dated June 1, 2016 (CJISD-ITS-DOC-08140-5 .5)

IT Support Services for City Technology

Engineering and Operations

This division designs, implements, operates, and supports technology solutions and resources in accordance with city wide architecture and governance. Responsibilities for this division include:

- Primary communications networks that provide public safety and constituent access to and from City government; the telephone system, the data network, and Public Safety Radio System. Responsible for sustaining all three systems operating as close to 100% availability as possible 24 hours a day, seven days a week.
- Design, acquisition, installation, maintenance, repair and management of fiber optic cables on behalf of City departments and approximately 20 other local, state and federal agencies.
- Procurement requests, allocation, operation and maintenance of city wide and departmental servers, virtual enterprise computing and SAN storage environments for large scale mission critical applications in a secure, reliable, 24/7 production environment for enterprise computing.
- Allocation, operation and maintenance of enterprise level services like messaging services, web access, file sharing, user management and remote access solutions.
- Collaborate with Enterprise Architecture team to develop standards for information technology equipment and software.
- Service Desk and technical support services for City's computers, peripherals, electronic devices and mobile device management.
- Centralized IT asset management to include research, procurement request, surplus and asset transfer.
- Facility management for a reliable production computing environment to the City departments.
- Support for other enterprise services and tools.

Compute System Technologies

This team manages the operations and maintenance of computing infrastructure, including servers, storage, backup and recovery, and enterprise support systems (e.g., Active Directory, VPN, etc.). The team is also responsible for safeguarding systems and data by performing required security patches, updates, and backups to ensure systems operate at as close to 100% availability as possible 24x7. Units within this group include:

Systems Operations. The team is focused on delivering the computing environment across multiple departments. The team has technical expertise to design, integrate, and operate a secure, reliable computing environment. Key technologies include Windows, Solaris, IBM AIX, and Linux.

Enterprise Services. Enterprise Services (ES) are large scale infrastructure and application services used by the City of Seattle end user community. This includes both SaaS and NGDC hosted infrastructure and application services. The team is responsible for EA vendor management, system administration, upgrades and technical support. Key technologies includes Microsoft Active Directory (AD), Distributed File System (DFS), Exchange Online, Office 365 and SharePoint Online infrastructure.

Infrastructure Tools. The team provides a single focus for the design, planning, deployment and maintenance of standard enterprise infrastructure monitoring and management tools. This includes system performance (Solarwinds, SCOM), configuration management (SCCM, WSUS), and monitoring and system management (Trend Micro, CRM, Vipre).

Virtual and Data Infrastructure. This team engineers and operates reliable, flexible, performant virtualized Windows, UNIX and Linux platforms and their related technologies in direct support of critical business applications. Key technologies include Solaris, Unix, Linux, Windows, and vmWare, and the associated virtualization Nutanix, IBM LPAR, and Solaris hardware.

The team also engineers and operates reliable, flexible, performant storage and data protection solutions to host and protect critical business data of all types, leveraging SAN, NAS, object, and cloud technologies. Key technologies include Dell Compellent, Quantum, Hitachi, NetApp, Cloud storage, Brocade fiber channel switching, and Commvault.

Network And Communications Technologies

This team is responsible for designing, installing, operating, and maintaining data, voice, radio, fiber optic, and structured cabling infrastructure that integrates with other technologies to provide access to resources used by City departments and the public we serve. Units within this group include:

> **Network Engineering & Operations.** The Network Services team engineers, operates and maintains the City's data network, including data center core networks, the internet perimeter, the network backbone, and local area networks that support systems and users across the City. This group designs, acquires, installs, maintains, repairs, and manages an enterprise data network that aligns with City architectures and standards. This group also participates in development of those standards and provides tier 2 and 3 end user support. This team supports technologies that include routing, switching, load balancing, enterprise Wi-Fi, DNS/DHCP/NTP, and network security (including firewalls, VPN appliances, certificate infrastructure, network access control, and web filtering.)

> **Telecommunication Engineering & Operations.** The Telecommunications Services team engineers, operates, and maintains a highly-reliable enterprise telephone and contact center infrastructure. This group supports end user move and change activity and provides tier 2 and 3 support. The Telecommunication Services team acquires, installs, maintains, and repairs telecommunications equipment and manages commercial telephony circuits. It supports technologies that include VoIP, circuit-switched telephony, voice mail, contact center services (including call routing scripts), audio conference bridges, commercial telephony services, SONET, and WDM.

> **Radio & Communications Infrastructure.** This team delivers radio services for public safety and other government departments. It provides extremely reliable infrastructure and support for end user mobile and portable radio equipment. The group installs and maintains communications equipment inside 911 dispatch centers and City vehicles, with primary support to SPD and SFD. The team also supports regional planning, maintenance, interoperability testing, and projects (including PSERN and Washington OneNet) in partnership with other local, state, and federal agencies. This team also designs, acquires, installs, maintains, repairs, and manages in-building structured

cabling systems and outside plant fiber optic and copper cable infrastructure for the City and approximately 20 external public agency partners. Technologies include trunked and conventional land mobile radio, microwave radio and other wireless communications systems (including point-to-multipoint and mesh networks,) distributed antenna systems, routing/MPLS, DS3/T1/DACS, outside plant cable infrastructure (including fiber and copper,) and structured cabling infrastructure.

End User Support

This team is responsible for providing a single point of contact for IT technical support, trouble ticket and service request resolution and referral services to other IT workgroups, and for communication for all changes, patches, upgrades and standards changes. The team is also responsible for providing technical support for the City's desktop computers, peripherals, electronic devices and mobile devices. Units within this group include:

Service Desk. The Service Desk team provides a single point of contact for Seattle IT services, promptly resolving incidents and service requests when first contacted whenever possible, escalating issues accurately and efficiently, and keeping users and partners aware of service status and changes.

Device Support. This team provides direct customer support for end user computing to all departments within the City and tier 2 escalation support and management of centralized end user computing applications and hardware.   requests.

Device Engineering. This team engineers and deploys software packages for end user applications, device drivers, patches, security updates and custom packages as required. This team evaluates and recommends hardware and software for end user standards. In addition, this team provides tier 3 escalation support and management of centralized end user computing applications and hardware.

Asset Management. This team is responsible tracking and inventory controls for city wide IT assets including desktops, laptops, printers, servers, switches, and miscellaneous Information Technology infrastructure. In addition to inventory control, the team will be forecasting replacement cycles for equipment based on City standards to promote a stable computing environment.

IT Operations Support

The IT Operations Support team is responsible for management of Information Technology facilities (including data centers and communications equipment rooms), and installation and cabling equipment within those facilities. This team provides the enterprise Network Operations Center (NOC) that monitors alerts, performs initial incident analysis, dispatches tier 2 and 3 technical support, and provides initial incident communication for network infrastructure and computing systems managed by Engineering and Operations. Units within this group include:

Installation Management. This team installs networking and computing equipment in data centers, communications rooms and wiring closets; installs and maintains network

cabling within data centers and equipment rooms according to City standards; and supports repair and end user move and change activity (including telephone move projects).

IT Operations Center. This team manages facilities which support City computing and communications services. This includes managing access to facilities, coordinating vendors, maintaining records (including data center inventory management), and, where applicable, monitoring facility systems (including CRUs, fire alarms, water detection sensors, UPS systems, and power consumption). This team also staffs the NOC that monitors alerts from network infrastructure and computing systems, performs initial problem analysis, dispatches appropriate tier 2 and 3 technical support team(s), and provides initial incident communication.

Application Services

This division designs, develops, integrates, implements, and supports application solutions in accordance with city wide architecture and governance. Its teams are organized to support business functions or service groups**.** The integration of application services will be completed gradually in 2017, with details of the organization and integration process still under development.

Applications

These teams will provide development and support for applications that include customer relationship management, billing, finance, human resources, work and asset management and records management.

Shared Platforms

These teams will provide development and support for applications that include engineering, spatial analysis, business intelligence, analytics, SharePoint Online and document management.

Cross Platform Services

These teams will provide support to application teams, including quality assurance, change control, database administration, integration services, and access management activities.

City of Seattle

Agency Information: Seattle PD - (WASPD0000)

Submitted By: Pepper Bojang-Jackson - On: March 22, 2017 Compliance Report with Agency Responses

Compliance Report

NCIC compliance standards must be improved and a response submitted to the WSP ACCESS Section.

Item:	1
Section Name:	Personnel Security
Question:	Are you maintaining a record of all your agency and/or county/city IT personnel that must receive a state of residency fingerprint background check within 30 days of employment? *(CJIS Security Policy, Version 5.5, Section 5.12.1.1)*
	Yes
	Please provide the SID numbers for all the IT personnel.
Agency Response:	List emailed 05/16/17

Item:	2
Section Name:	Personnel Security
Question:	Have all your agency and/or county/city IT personnel viewed the technical security awareness training (Level 4) in CJIS Online? *(CJIS Security Policy, Version 5.5, Section 5.2)*
	Yes
	All technical staff must view the technical security training - level 4 once every two years. Please provide a list of names of who viewed the training. The training is available at the following address: https://www.cjisonline.com/
Agency Response:	Sent email 05/16/17

Item:	3

Section Name: Personnel Security

Question: Does your agency use an IT vendor for any IT needs?

Sub Question(s)

Item: 3.1

Section Name: Personnel Security

Question: Have all IT _vendors_ had a Washington State fingerprint background check completed? *(CJIS Security Policy, Version 5.5, Section 5.12.1.1 and 5.12.1.2)*

User Answer: Yes

Compliance Response: All IT vendors must have a Washington State fingerprint
background

check completed.

Agency Response: List emailed 05/16/17

Sub Question(s)

Item: 3.2

Section Name: Personnel Security

Question: Please send a copy of the security addendum signed by each employee of the vendor company to CJISAudits@wsp.wa.gov

User Answer: I have read and will comply.

Compliance Response: Please provide a copy of the signed security addendum for each employee of the vendor company. I am missing security addendums for the following vendors:

1. 4quarters
2. Advantage Factory
3. Dorsey Consulting
4. Gartner
5. Genetec Corp
6. Sabey
7. Sysorex Consulting
8. TASER
9. TEKsystems
10. Versaterm - only a few

Agency Response: 1. 4quarters - Emailed 05/08/17
2. Advantage Factory - All Advantage Factory accounts are inactive

3. Dorsey Consulting - DOJ Monitoring Team - Should be
CJIS Level 2, not 4 (deactivated all accounts)
4. Emailed 05/22/17
5. Genetec Corp - All accounts are inactive.
6. Adashi - Adashi employees are working in an environment
that does not currently have CJIS data. Future plans do
include CJIS data so they are in the process of completing the
Security Addendums.
7. Sysorex Consulting - All accounts are inactive

8. TASER - Emailed 05/18/17
9. TEKsystems - Contractor is now City IT w/updated information.
10. Versaterm - Emailed 05/08/17

Item:	4
Section Name:	System and Communications Protection and Information Integrity
Question:	Does your agency email CJI? *(CJIS Security Policy, Version 5.5, Section 5.10.1.2)*

Sub Question(s)

Item:	4.1
Section Name:	System and Communications Protection and Information Integrity
Question:	Is the email that contains CJI encrypted? *(CJIS Security Policy, Version 5.5 Section 5.10.1.2)*
User Answer:	No
Compliance Response:	CJI that is emailed is required to be encrypted. Please advise when you will have this in place.
Agency Response:	Seattle is utilizing Office 365 for email and email is encrypted

Is the email encrypted in transit? https://products.office.com/en-us/business/office-365-trust-center-security

Outlook client to O365 - SSL/TLS connection is established between Outlook client and O365

O365 to OME server - SSL / TLS connection between EXO Transport servers and OME server. "Office 365 uses Transport Layer Security (TLS) to encrypt the connection, or session, between two servers." https://support.office.com/en-us/article/Email-encryption-in-Office-365- c0d87cbe-6d65-4c03-88ad-5216ea5564e8

Is the email encrypted at rest when it sits on the server? https://support.office.com/en-us/article/Email-encryption-in-Office-365-c0d87cbe-6d65-4c03-88ad-5216ea5564e8

What about encryption for data at rest?

"Data at rest" refers to data that isn't actively in transit. In Office 365, email data at rest is encrypted using BitLocker Drive Encryption.
BitLocker encrypts the hard drives in Office 365 datacenters to provide enhanced protection against unauthorized access. To learn more, see BitLocker Overview.

What level of encryption does OME use? - Microsoft attests that they meet and/or exceed FBI CJIS requirements

The CJIS Security Policy defines 13 areas that private contractors such as cloud service providers must evaluate to determine if their use of cloud services can be consistent with CJIS requirements. These areas correspond closely to NIST 800-53, which is also the basis for the Federal Risk and Authorization Management Program (FedRAMP), a program under which Microsoft has been certified for its Government Cloud offerings

Item:	5
Section Name:	Event Logging
Question:	Does your agency have an established audit trail capable of monitoring the following: - Successful and unsuccessful log on attempts - Successful and unsuccessful password changes - Successful and unsuccessful attempts to access, create, write, delete or change permissions on a user account, file, directory or other system resources - Successful and unsuccessful actions by privileged accounts - Successful and unsuccessful attempts for users to access, modify, or destroy audit log files (CJIS Security Policy, Version 5.5, Section 5.4.1.1)
User Answer:	No
Compliance Response:	Please advise when your agency will have an established audit trail capable of monitoring the following: - Successful and unsuccessful log on attempts - Successful and unsuccessful password changes - Successful and unsuccessful attempts to access, create, write, delete or

change permissions on a user account, file, directory or other system resources

- Successful and unsuccessful actions by privileged accounts
- Successful and unsuccessful attempts for users to access, modify, or destroy audit log files

Agency Response:

Seattle PD has established an audit trail capable of monitoring the following:

- Successful and unsuccessful log on attempts
- Successful and unsuccessful password changes
- Successful and unsuccessful attempts to access, create, write, delete or change permissions on a user account, file, directory or other system resources
- Successful and unsuccessful actions by privileged accounts
- Successful and unsuccessful attempts for users to access, modify, or destroy audit log files

---

Item:	6
Section Name:	Identification and Authentication
Question:	Does your agency and/or county/city IT department employee perform remote assistance from a non-secure location? Example employees home or coffee shop etc. *(CJIS Security Policy, Version 5.5, Section 5.6.2.2)*
User Answer:	Yes
Compliance Response:	IT has the ability to remote in the system from a non-secure location. Please advise once Advanced Authentication will be in place or when a remote session will be virtually escorted at all times.
Agency Response:	

Full policy emailed to ACCESS on 04/23/18:

This policy applies to employees, contractors, or vendors who have a need to remotely access the CJI (Criminal Justice Information) in-scope systems for maintenance and operations. All access both remote and within the Seattle network (except for the SPD network) is through bastion hosts protected by two-factor Advanced Authentication (AA).

*All non-law enforcement personnel who perform criminal justice functions or have access to Criminal justice data shall acknowledge, via signing of the CJIS Security Addendum Certification page, and abide by all aspects of the CJIS

Security Addendum. Seattle Information Technology employees are not required to sign the Security Addendum provided there is a CJIS Management Control Agreement (MCA) between Seattle Information Technology and Seattle Police/Fire.

*CJIS Security Awareness Training shall be required upon initial assignment, and biennially thereafter, for all personnel who have access toCJI.

Verify Identification: a state of residency and national fingerprint-based record checks shall be conducted (prior to) assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI.

*All requests for access shall be made as specified by the CSO. The CSO, or their designee, is authorized to approve access to CJI. All designees shall be from an authorized criminal justice agency.

*VPN access must be approved by the requesting department prior to activation.

*Users must not:

Type remote access passwords while someone is watching. Users shall directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. (CJIS Security Policy Section 5.5.5) A session lock is not a substitute for logging out of the information system or from disconnecting a remote session.

Be connected to other network connections during remote access sessions into CJI data in-scope (e.g., no split tunnels are allowed).

*Users must maintain current virus protection and a host firewall on remote systems to protect from viruses and other remote attacks.

*Vendors must:

Be provided with the minimum access required to perform the necessary duties while the VPN session is active. Other access and privileges will be limited to the specific function performed by each vendor or service provider.

Be monitored by a City of Seattle CDE administrator during an assisted remote control session using Skype for Business or other current City of Seattle Enterprise standard for remote control sessions. The CDE administrator must have the ability to end the session at any time and the session must be terminated as soon as their work has finished.

Item:	6.1
Section Name:	Identification and Authentication
Question:	Describe the type of Advanced Authentication (AA) that is being used while the remote session is in process or advise if the session is being virtually escorted at all times. Virtually escorting is permitted when the following conditions are met:

- The session shall be monitored at all times by an authorized escort.
- The escort shall be familiar with the system/area in which the work is being performed.
- The escort shall have the ability to end the session at any time.
- The remote administrative personnel connection shall be via an encrypted (FIPS 140-2 certified) path.
- The remote administrative personnel shall be identified prior to access and authenticated prior to or during the session. This authentication may be accomplished prior to the session via an Advanced Authentication (AA) solution or during the session via active teleconference with the escort throughout the session.

(CJIS Security Policy, Version 5.5, Section 5.5.6)

User Answer:	Certificate on the workstation. RSA is being implemented for network equipment.
	Rarely workstations are remotely accessed. If they are, an SPD computer would be used to do the support work.
Compliance Response:	Please advise when AA will be in place for IT staff that conducts remote assistance on applications or networks that access CJI or when all personnel will be virtually escorted or a policy prohibiting remote access from an unsecure location is established.
Agency Response:	See #6

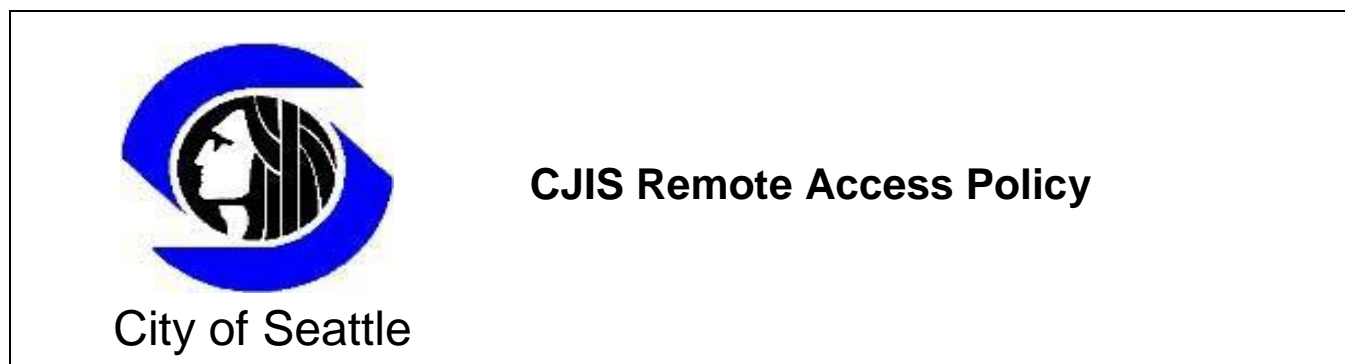| Item:	7
Section Name:	Cloud Computing
Question:	Does the agency utilize a cloud provider to host or store CJI related systems, applications or data? *(CJIS Security Policy, Version 5.5, Section 5.10.1.5)*

↳ Sub Question(s)

Item:	7.1
Section Name:	Cloud Computing
Question:	Is the CJI encrypted prior to entering the cloud?

User Answer:	No
Compliance Response:	Please advise when the CJI that goes to the cloud will be encrypted.
Agency Response:	Seattle is utilizing Office 365 and CJI is encrypted

Report Summary:

The Federal Bureau of Investigation (FBI) assigned the Washington State Patrol (WSP) as the Criminal Justice Information Services (CJIS) Systems Agency (CSA) for the state of Washington. The CSA is responsible for establishing and administering an information technology security program throughout the CSA user community, to include the local levels. All standards set forth in the audit questionnaire originate

from the CJIS Security Policy which provides Criminal Justice Agencies (CJA) with a minimum set of security requirements for access to FBI CJIS Division systems and information to protect and safeguard Criminal Justice Information (CJI). This minimum standard of security requirements ensures continuity of information protection. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit.

Remote Access Policy

CJIS Remote Access Policy

City of Seattle

June 1st, 2018

Overview

The CJI Remote Access Policy defines the necessary controls for remote access to Criminal Justice Information Services (CJIS) in scope systems.

Purpose

This policy ensures proper measures are taken when granting remote access to any employee, contractor, or vendor, to Criminal Justice Information (CJI) in-scope systems.

Definition

CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, decimation, storage, and destruction of CJI.

Scope and Applicability

This policy applies to personnel at City of Seattle, including those affiliated with third parties who remotely access City of Seattle systems to include CJI data. The policy applies to all systems owned by and/or administered by City of Seattle, including network to network VPN tunnels.

Policy

This policy applies to City of Seattle employees, City of Seattle Police Department employees, contractors, or vendors who have a need to remotely access the CJI (Criminal Justice Information) in-scope systems for maintenance and operations. All access both remote and within the City of Seattle network or Public network, are required to utilize two factor authentication & VPN tunnel on City of Seattle workstation OR through a jump-box protected by two-factor Advanced Authentication (AA). Contractors, Vendors and City employees accessing in-scope systems from non-city computers are required to utilize the jump-box AA solution.

All non-law enforcement personnel who perform criminal justice functions or have access to Criminal justice data shall acknowledge, via signing of the CJIS Security Addendum Certification page, and abide by all aspects of the CJIS Security Addendum. Seattle Information Technology employees are not required to sign the Security Addendum provided there is a CJIS Management Control Agreement (MCA) between Seattle Information Technology and Seattle Police/Fire.

- CJIS Security Awareness Training shall be required upon initial assignment, and biennially thereafter, for all personnel who have access to CJI.
- Verify Identification: a state of residency and national fingerprint-based record checks shall be conducted (prior to) assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI.
- All requests for access shall be made as specified by the CSO (CJIS Systems Officer). The CSO, or their designee, is authorized to approve access to CJI. All designees shall be from an authorized criminal justice agency.
- VPN access must be approved by the requesting department prior to activation.
- Users must not:
  - Type remote access passwords while someone is watching. Users shall directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. (CJIS Security Policy Section 5.5.5) A session lock is not a substitute for logging out of the information system or from disconnecting a remote session.
  - Be connected to other network connections during remote access sessions into CJI data in-scope (e.g., no split tunnels are allowed).
- Users must maintain current virus protection and a host firewall on remote systems to protect from viruses and other remote attacks.
- Vendors must:
  - Be provided with the minimum access required to perform the necessary duties while the VPN session is active. Other access and privileges will be limited to the specific function performed by each vendor or service provider.
  - Be monitored by a City of Seattle CDE administrator during an assisted remote control session using Skype for Business or other current City of Seattle Enterprise standard for remote control sessions. The CDE administrator must have the ability to end the session at any time and the session must be terminated as soon as their work has finished.

Applicability of other Policies

January 17, 2016 1 The City of Seattle has an existing Remote Access Policy that must be adhered to and can be found [here](#).

Enforcement

Enforcement of this policy will be led by the Chief Technology Officer (CTO). Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment or vendor contract termination. Where illegal activities or loss of City of Seattle assets are known or suspected, the City of Seattle must report activities to the appropriate authorities, City of Seattle is obliged to adhere to breach reporting by statutory limitation and must notify the Terminal Agency Coordinator (TAC) of any potential violations. All potential violations that involve CJI must be report to the Washington State Patrol ACCESS Section.

Implementation

This Policy is implemented by the ITD Security, Risk, and Compliance Director and applies to the City of Seattle access to CJI.

Document Control

Version	Content	Contributors	Approval Date
1.0	Initial Draft	Reviews: Denise Mendoza; Pepper Bojang-Jackson Approvers: CISO Andrew Whitaker CTO	
1.1	Initial Draft	Reviews: Denise Mendoza; Pepper Bojang-Jackson	
1.2	Initial Draft	Reviews: Denise Mendoza Bruce Hills Pepper Bojang-Jackson	
1.3	Review	Andrew Whitaker	6/5/18
1.4	Approved	Tracye Cantrell	6/12/18

Appendix L: CTO Notification of Surveillance Technology

Thank you for your department's efforts to comply with the new Surveillance Ordinance, including a review of your existing technologies to determine which may be subject to the Ordinance. I recognize this was a significant investment of time by your staff; their efforts are helping to build Council and public trust in how the City collects and uses data.

As required by the Ordinance (SMC 14.18.020.D), this is formal notice that the technologies listed below will require review and approval by City Council to remain in use. This list was determined through a process outlined in the Ordinance and was submitted at the end of last year for review to the Mayor's Office and City Council.

The first technology on the list below must be submitted for review by March 31, 2018, with one additional technology submitted for review at the end of each month after that. The City's Privacy Team has been tasked with assisting you and your staff with the completion of this process and has already begun working with your designated department team members to provide direction about the Surveillance Impact Report completion process.

Please let me know if you have any questions.

Thank you,

Michael Mattmiller

Chief Technology Officer

Technology	Description	Proposed Review Order
Automated License Plate Recognition (ALPR)	ALPRs are computer-controlled, high-speed camera systems mounted on parking enforcement or police vehicles that automatically capture an image of license plates that come into view and converts the image of the license plate into alphanumeric data that can be used to locate vehicles reported stolen or otherwise sought for public safety purposes and to enforce parking restrictions.	1
Booking Photo Comparison Software (BPCS)	BCPS is used in situations where a picture of a suspected criminal, such as a burglar or convenience store robber, is taken by a camera. The still screenshot is entered into BPCS, which runs an algorithm to compare it to King County Jail booking photos to identify the person in the picture to further investigate his or her involvement in the crime. Use of BPCS is governed by SPD Manual §12.045.	2
Forward Looking Infrared Real-time video (FLIR)	Two King County Sheriff's Office helicopters with Forward Looking Infrared (FLIR) send a real-time microwave video downlink of ongoing events to commanders and other decision-makers on the ground, facilitating specialized radio tracking equipment to locate bank robbery suspects and provides a platform for aerial photography and digital video of large outdoor locations (e.g., crime scenes and disaster damage, etc.).	3

Technology	Description	Proposed Review Order
Undercover/ Technologies	The following groups of technologies are used to conduct sensitive investigations and should be reviewed together. • **Audio recording devices**: A hidden microphone to audio record individuals without their knowledge. The microphone is either not visible to the subject being recorded or is disguised as another object. Used with search warrant or signed Authorization to Intercept ([RCW 9A.73.200](#)). • **Camera systems**: A hidden camera used to record people without their knowledge. The camera is either not visible to the subject being filmed or is disguised as another object. Used with consent, a search warrant (when the area captured by the camera is not in plain view of the public), or with specific and articulable facts that a person has or is about to be engaged in a criminal activity and the camera captures only areas in plain view of the public. • **Tracking devices**: A hidden tracking device carried by a moving vehicle or person that uses the Global Positioning System to determine and track the precise location. U.S. Supreme Court v. Jones mandated that these must have consent or a search warrant to be used.	4
Computer-Aided Dispatch (CAD)	CAD is used to initiate public safety calls for service, dispatch, and to maintain the status of responding resources in the field. It is used by 911 dispatchers as well as by officers using mobile data terminals (MDTs) in the field.	5

Technology	Description	Proposed Review Order
CopLogic	System allowing individuals to submit police reports on-line for certain low-level crimes in non-emergency situations where there are no known suspects or information about the crime that can be followed up on. Use is opt-in, but individuals may enter personally-identifying information about third-parties without providing notice to those individuals.	6
Hostage Negotiation Throw Phone	A set of recording and tracking technologies contained in a phone that is used in hostage negotiation situations to facilitate communications.	7
Remotely Operated Vehicles (ROVs)	These are SPD non-recording ROVs/robots used by Arson/Bomb Unit to safely approach suspected explosives, by Harbor Unit to detect drowning victims, vehicles, or other submerged items, and by SWAT in tactical situations to assess dangerous situations from a safe, remote location.	8
911 Logging Recorder	System providing networked access to the logged telephony and radio voice recordings of the 911 center.	9
Computer, cellphone and mobile device extraction tools	Forensics tool used with consent of phone/device owner or pursuant to a warrant to acquire, decode, and analyze data from smartphones, tablets, portable GPS device, desktop and laptop computers.	10
Video Recording Systems	These systems are to record events that take place in a Blood Alcohol Concentration (BAC) Room, holding cells, interview, lineup, and polygraph rooms recording systems.	11
Washington State Patrol (WSP) Aircraft	Provides statewide aerial enforcement, rapid response, airborne assessments of incidents, and transportation services in support of the Patrol's public safety mission. WSP Aviation currently manages seven aircraft equipped with FLIR cameras. SPD requests support as needed from WSP aircraft.	12

Technology	Description	Proposed Review Order
Washington State Patrol (WSP) Drones	WSP has begun using drones for surveying traffic collision sites to expedite incident investigation and facilitate a return to normal traffic flow. SPD may then request assistance documenting crash sites from WSP.	13
Callyo	This software may be installed on an officer's cell phone to allow them to record the audio from phone communications between law enforcement and suspects. Callyo may be used with consent or search warrant.	14
I2 iBase	The I2 iBase crime analysis tool allows for configuring, capturing, controlling, analyzing and displaying complex information and relationships in link and entity data. iBase is both a database application, as well as a modeling and analysis tool. It uses data pulled from SPD's existing systems for modeling and analysis.	15
Parking Enforcement Systems	Several applications are linked together to comprise the enforcement system and used with ALPR for issuing parking citations. This is in support of enforcing the Scofflaw Ordinance SMC 11.35.	16
Situational Awareness Cameras Without Recording	Non-recording cameras that allow officers to observe around corners or other areas during tactical operations where officers need to see the situation before entering a building, floor or room. These may be rolled, tossed, lowered or throw into an area, attached to a hand-held pole and extended around a corner or into an area. Smaller cameras may be rolled under a doorway. The cameras contain wireless transmitters that convey images to officers.	17
Crash Data Retrieval	Tool that allows a Collision Reconstructionist investigating vehicle crashes the opportunity to image data stored in the vehicle's airbag control module. This is done for a vehicle that has been in a crash and is used with consent or search warrant.	18

Technology	Description	Proposed Review Order
Maltego	An interactive data mining tool that renders graphs for link analysis. The tool is used in online investigations for finding relationships between pieces of information from various sources located on the internet.	19

Please let me know if you have any questions.

Thank you,

Michael

Appendix M: Criminal Justice Information Services (CJIS) Policy Documentation

Retroactive Technology Request By: SEATTLE POLICE DEPARTMENT

Appendix M: Criminal Justice Information Services (CJIS) Policy Documentation | Surveillance Impact Report | 911 LOGGING RECORDER |page 63