

Group 4A Surveillance Impact Reports (SIRs):

SPD Audio Recording Systems (CB 120307)

SPD Maltego (CB 120308)

SPD IBM i2 iBase (CB 120309)

Economic Development, Technology & City Light Committee

April 27, 2022

SIR Overview Process

Jim Loter, Interim Chief Technology Officer

Sarah Carrier, Privacy Program Manager

Surveillance Criteria

Definition: *Technology whose primary purpose is to observe or analyze the movements, behavior, or actions of identifiable individuals in a manner that is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice. Identifiable individuals also include individuals whose identity can be revealed by license plate data when combined with any other record.*

Exclusions

- Consents to provide the data
- Opt-out notice
- Body-worn cameras
- Police vehicle cameras
- Cameras installed pursuant to state law...or to record traffic violations
- Security cameras
- City infrastructure protection cameras
- Technology that monitors only City employees

Inclusions

- Disparately impacts disadvantaged groups
- PII shared with non-City entities that will use the data for a purpose other than providing the City with a contractually agreed-upon service
- Collects data that is personally identifiable even if obscured, de-identified, or anonymized after collection
- Raises reasonable concerns about impacts to civil liberty, freedom of speech or association, racial equity, or social justice

Surveillance Impact Report (SIR) Process

- Submitted for all retroactive and newly proposed technologies that meet the definition and have no exclusion criteria
- Created by the Departments with project management from IT

1

Privacy Impact Assessment

2

Financial Information

3

Racial Equity Toolkit

4

Public Engagement Comments and Analysis

5

Privacy and Civil Liberties Impact Assessment

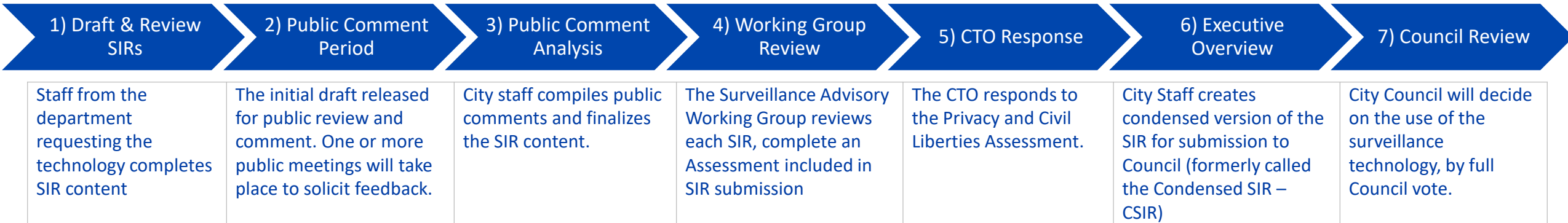
6




CTO Response

7

Appendices & Supporting Documentation

General SIR Creation Timeline



Group	Depts.	28 Technologies (16 Completed)		Council Bill	Status
Group 1 (2)	SDOT	<ul style="list-style-type: none"> License Plate Readers Closed Circuit Television Equipment "Traffic Cameras" 		CB 119519 CB 119519	Completed
Group 2 (9)	SCL SFD SPD	<ul style="list-style-type: none"> Binoculars/Spotting Scope Check Meter Device SensorLink Amp Fork Computer-Aided Dispatch 911 Logging Recorder Automated License Plate Reader Parking Enforcement Systems including Automated License Plate Reader Computer-Aided Dispatch CopLogic 		CB 120002 CB 120002 CB 120002 CB 120003 CB 120024 CB 120025 CB 120026 CB 120027 CB 120028	Completed
Group 3 (3)	SPD	<ul style="list-style-type: none"> Forward Looking Infrared Real-time video (FLIR) Situational Awareness Cameras Without Recording Video Recording Systems 		CB 120053 CB 120054 CB 120055	Completed
Group 4A (7)	SFD SDOT SPD	<ul style="list-style-type: none"> Emergency Scene Cameras, Hazmat Camera *Acyclica Audio Recording Systems Maltego IBM i2 iBase *Callyo 		CB 120171 Memo CB 120307 CB 120308 CB 120309	Completed 9/15/21, 1/4/22 4/27 EDTCL 4/27 EDTCL 4/27 EDTCL
Group 4B (7)	SPD	<ul style="list-style-type: none"> Camera systems; Tracking Devices; Remotely Operated Vehicles (ROVs); Hostage Negotiation Throw Phone; Crash Data Retrieval; GeoTime; Computer, cellphone and mobile device extraction tools 			Public Engagement Process

Group 4A SIR Public Engagement

- Group 4a Surveillance Technologies Public Meetings on June 10th, 2021 & July 20th, 2021
- One Page Flyers
- Online Public Comment Meeting
 - Recorded and posted online

Engagement Method	(Approximate) Number of Individuals Participating	Number of Comments Received	Number of Questions Received
Public Meeting	13	-	8
Online Comments	13	13	-
Letters	2	2	-
Total	28	15	8

Seattle Police Department Group 4A SIRs

SPD Audio Recording Systems

SPD Maltego

SPD IBM i2 iBase

Capt. James Britt, SPD

Seattle Police Department Mission

- Prevent crime;
- Enforce the law; and
- Support quality public safety by delivering respectful, professional and dependable police services.

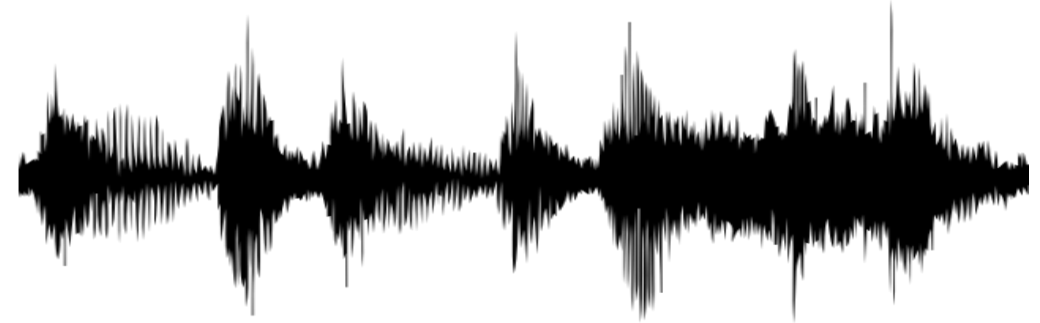
Audio Recording Systems

What is the technology?

- Audio recording devices are typically known as “wires” and can be concealed on a person or hidden in or on objects within a particular environment.
- Audio recording devices must be turned on by an individual and they record only portions of a conversation that occur while the device is on.

Why do we use the technology?

- Audio recording systems contribute to crime reduction by assisting in collecting evidence related to serious and/or violent criminal activity as part of the investigation of criminal activity.
- Audio recording systems allow SPD to pursue resolution of criminal investigations expeditiously by recording conversations of suspects, once an appropriate determination that sufficient probable cause exists has been made and a warrant has been issued.



Audio Recording Systems

Data Collection

- All audio recording systems utilized by SPD are managed and maintained with the Technical and Electronic Support Unit (TESU).
- Data collected from audio recording devices is provided to the requesting Officer/Detective for inclusion in the investigation file and is stored following evidence guidelines.

Protections

- Audio recording devices are utilized only after legal standards of consent and/or court-issued warrant have been met, as required by the Washington Privacy Act, Chapt. 9.73 RCW.
- Deployment of audio recording devices is constrained to the conditions stipulated by consent and/or court order, which provides the legal authority and the scope of collection.
- All deployments of audio recording devices are documented by TESU and subject to audit by the Office of Inspector General and the federal monitor at any time.

Audio Recording Systems

Related Policies

- Washington Privacy Act, Chapt.9.73 RCW
- SPD Policy 5.001 – Standards and Duties
- SPD Policy 5.002 – Responsibilities of Employees Concerning Alleged Policy Violations
- SPD Policy 5.140 – Bias-Free Policing
- SPD Policy 6.060 – Collection of Information for Law Enforcement Purposes
- SPD Policy 7.010 – Submitting Evidence
- 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
- SPD Policy 12.111 – Use of Cloud Storage Services

Maltego

What is the technology?

- Maltego is an Open-Source Intelligence (OSINT) platform which presents publicly available information in an easy to interpret visual entity-relationship model which allows investigators to analyze connections between individuals related to criminal investigations.
- Maltego queries public data on the internet, such as domains, and displays it in a diagram showing links.



Why do we use the technology?

- Maltego is a popular tool that is used across the information-security community for both defensive cyber-security programs and for investigating breaches and instances of cyber-crime.
- A useful tool used in cyber-crime investigations, as these incidents often involve interactions between individuals, devices, and networks that are otherwise unknown.

Maltego

Data Collection

- Maltego queries publicly available data on the internet and collects information based on the parameters of the search request entered by a detective, much like Google returns results based on specific search terms.
- SPD utilizes Maltego to investigate cybercrimes, primarily in determining the digital origin of attacks against cyber infrastructure.

Protections

- Access to Maltego is restricted to use for the related security incident and/or pertinent criminal investigations and subject to Department Policy regarding ongoing criminal investigations.
- Maltego is used by two trained TESU detectives within TESU, and by no other entity. Use of Maltego is governed by SPD Policy, the City of Seattle Intelligence Ordinance, 28 CFR Part 23, and CJIS requirements.

Maltego

Related Policies

- Washington Privacy Act, Chapt.9.73 RCW
- SPD Policy 5.001 – Standards and Duties
- SPD Policy 5.002 – Responsibilities of Employees Concerning Alleged Policy Violations
- SPD Policy 5.140 – Bias-Free Policing
- SPD Policy 6.060 – Collection of Information for Law Enforcement Purposes
- SPD Policy 7.010 – Submitting Evidence
- 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
- SPD Policy 12.111 – Use of Cloud Storage Services
- City of Seattle Intelligence Ordinance, 28 CFR Part 23

IBM i2 iBase

What is the technology?

- i2 iBase is a link analysis software used to combine data stored in SPD criminal information systems with information gathered during criminal investigations and display that information on a link chart.
- A virtual “pin board,” helping investigators to visualize the connections between known entities, vehicles, locations, etc. in the course of a criminal investigation.

Why do we use the technology?

- IBM i2 iBase is used by analysts within the Real Time Crime Center (RTCC) to assist with criminal investigations and to provide actionable information to units in the field.
- Visualizing criminal information provides investigators a more thorough understanding of complicated criminal investigations.



IBM i2 iBase

Data Collection

- The iBase application imports specific data elements related to the investigation from SPD's Records Management System (RMS) and Computer Aided Dispatch (CAD) system.
- Users may also manually add additional information that they have collected during the course of a criminal investigation to assist in understanding complex investigations.

Protections

- Only authorized users can access the system, technology, or the data. Access to the iBase system requires SPD personnel to log in with password-protected login credentials. All of these employees are ACCESS and Criminal Justice Information System (CJIS) certified.
- The I2 iBase system is CJIS compliant. The software also logs user sign on/off, each time a user accesses any piece of data, and any additions or changes a user makes.

IBM i2 iBase

Related Policies

- Washington Privacy Act, Chapt.9.73 RCW
- SPD Policy 5.001 – Standards and Duties
- SPD Policy 5.002 – Responsibilities of Employees Concerning Alleged Policy Violations
- SPD Policy 5.140 – Bias-Free Policing
- SPD Policy 6.060 – Collection of Information for Law Enforcement Purposes
- SPD Policy 7.010 – Submitting Evidence
- 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
- SPD Policy 12.111 – Use of Cloud Storage Services
- City of Seattle Intelligence Ordinance, 28 CFR Part 23

Questions