SEATTLE CITY COUNCIL
CENTRAL STAFF

February 25, 2021

M E M O R A N D U M

To: Transportation and Utilities Committee
From: Lise Kaye, Analyst
Subject: Council Bill 120004 Seattle Police Department Surveillance Technologies

On Wednesday, March 3, 2021 the Transportation and Utilities Committee will discuss Council Bill (CB) 120004. The proposed bill is intended to meet the requirements of Seattle Municipal Code Chapter 14.18, Acquisition and Use of Surveillance Technologies.[1] (Attachment 1 to this memo summarizes these requirements and the process by which the Executive develops the required Surveillance Impact Reports.) The proposed bill would approve the Seattle Police Department's (SPD's) continued use of the following technologies:

1. **Automated License Plate Readers**
2. **Parking Enforcement System**
3. **Computer-Aided Dispatch**
4. **CopLogic**
5. **911 Logging Recorder**

Passage of the bill would also accept the Surveillance Impact Reports (SIRs) for these technologies, as further detailed in each section of this memo. As required by SMC 14.18.020(3), the Executive conducted a public engagement process to receive public comments and/or concerns about this technology. In addition, the Community Surveillance Working Group ("Working Group") has completed a Privacy and Civil Liberties Impact Assessment ("Impact Assessment") of the technology, and the City's Chief Technology Officer (CTO) has provided his response ("Response") to the Impact Assessment.

This memo provides summaries of each of the five SIRs in the order listed above. Each summary includes a brief synopsis of the potential civil liberties impacts from the technology and the public engagement processes for each, as reported in the SIRs. The summaries also describe concerns and recommendations from the Working Group's Impact Assessments and the CTO's Response. Finally, each section identifies policy considerations for possible Council action.

Committee Action

Options for Council action are as follows:

1. Pass CB 120002, 120003 and/or 120004 as transmitted;
2. Request Central Staff to prepare amendments to the Council Bill and/or to one or more of the SIRs to address additional concerns or issues; or
3. Take no action.

[1] (Ord. 125679 , § 1, 2018; Ord. 125376 , § 2, 2017.)

1. Automated License Plate Readers

CB 120004 would approve SPD's continued use of and accept the SIR for Automated License Plate Readers, which employ a combination of high definition infrared digital cameras (Neology PIPs) and locational software (Neology Back Office System Software, or "BOSS"). SPD uses Automated License Plate Readers to check a vehicle against a "HotList" of license plate numbers from the Washington Crime Information Center, the FBI's National Crime Information Center, and SPD's investigations to identify stolen vehicles, and vehicles wanted in conjunction with felonies or associated with wanted persons or Amber and Silver Alerts (abducted children and missing people). Officers must verify that the system accurately read the license plate and ask Dispatch to verify that a vehicle is listed as stolen before taking any action. SPD retains data from Automated License Plate Readers for 90 days, or in investigative files, for the retention period related to the incident in question.

SPD Policy 16.170 directs that Automated License Plate Readers are only to be used for the following purposes:

- Locating stolen vehicles;
- Locating stolen license plates;
- Locating wanted, endangered or missing persons; or those violating protection orders;
- Canvassing the area around a crime scene;
- Locating vehicles under SCOFFLAW[2]; and
- Electronically chalking vehicles for parking enforcement purposes.

SPD Policy 16.170 also limits access to data maintained on the Back Office System Software to the following purposes:

- Search of specific or partial plate(s) and/or vehicle identifiers as related to:
- A crime in-progress;
- A search of a specific area as it relates to a crime in-progress;
- A criminal investigation; or
- A search for a wanted person; or
- Community caretaking functions such as, locating an endangered or missing person.
- Officers/detectives conducting searches in the system will complete the Read Query screen documenting the justification for the search and applicable case number.

Civil Liberties and Potential Disparate Impacts on Historically Marginalized Communities

Departments submitting a SIR are required to complete an adapted version of the Racial Equity Toolkit (RET) to inform the SIR public engagement process and to highlight and mitigate impacts on racial equity from the use of the technology. The RET for the Automated License Plate

[2] See Ordinance 124558 relating to vehicle immobilization due to unpaid tickets for parking infractions

Readers identifies a potential civil liberties impact as the risk that, without appropriate policy, license plate data could be used to identify individuals without reasonable suspicion of having committed a crime or to search for information that is not incidental to any active investigation. The RET also cites the potential concern that SPD would over-surveil vulnerable or historically targeted communities, deploying the Automated License Plate Reader to diverse neighborhoods more often than to other areas of the City.

In response to concerns expressed during development of the SIR, SPD updated its relevant policies (SPD Policy 16.170) in January 2019 by adding definitions of the terms used in the operation of the Automated License Plate Reader technology, detailing authorized and prohibited uses, expanding on the required training for employees prior to access and use, defining response to alerts, detailing how Automated License Plate Reader equipment is to be handled, detailing data storage and retention, and detailing policy around the release or sharing of Automated License Plate Reader data. SPD also updated its policy related to Foreign Nationals, emphasizing that SPD has no role in immigration enforcement and will not inquire about any person's immigration status. The RET states that response to these updated policies will be "compiled and analyzed" as part of the CTO's annual equity assessments.

Public Engagement

The Executive accepted public comments on this technology from October 8, 2018 through November 5, 2018 and conducted three public meetings to solicit public comment on this SIR and the SIR for SPD's Parking Enforcement Systems on October 22, 29 and 30, 2018. In addition, the Department of Neighborhoods conducted two focus groups on November 8 and November 20, 2018. Appendix B in the SIR includes a statistical analysis of public comments (specific to Automated License Plate Readers) and demographics (including all Group 1 SIR Comments); Appendix E contains comments and survey results received from members of the public, some which expressed support for this technology and others expressing a wide range of privacy concerns, including with respect to surveillance overall; Appendix F contains letters from three organizations concerned about issues including use of data, data retention, data sharing and transparency; and Appendix G contains letters submitted from the public expressing concern about surveillance in general and about issues including data access, retention, sharing, and transparency.

Privacy and Civil Liberties Impact Assessment – Automated License Plate Reader

The Working Group's Impact Assessment identifies eight concerns about the allowable use of data, data access, collection, retention and sharing, system audits, the relation of this technology and the effectiveness of the technology in solving crimes.[3] It also recommends that Council adopt five specific policies. The following sections summarize the CTO's Response to the concerns and describe whether and how the SIRs as drafted would address the Working Group's recommended policies.

[3] The Impact Assessment states that the SIR does not include the new policies or indicate whether the new policies have been adopted by SPD. However, the updated SIR states that the new SPD Automated License Plate Reader policy went into effect on February 1, 2019 and references to the new policy are noted in the updated SIR next to the original policy references.

Key Concerns and the CTO's Response. Table 1 summarizes CTO's response to each of the Working Group's concerns. The Response concludes that SPD's updated policy, training and limitations from the technology itself provide adequate mitigation for the potential privacy and civil liberty concerns raised by the Working Group.

Table 1. CTO Response to Privacy and Civil Liberties Impact Assessment of SPD's Automated License Plate Reader Technology

Working Group Concern	CTO Response
1. Does not impose meaningful restrictions on the purposes for which Automated License Plate Reader data may be collected or used	SPD Policy outlines the specific situations or use cases that Automated License Plate Reader can be both used for and under which the data can be accessed.[4] The specific limitations on use preclude a scenario of "dragnet" use where Automated License Plate Reader is constantly in use as a patrol vehicle moves throughout the City.
2. Does not justify SPD's 90-day retention period.	SPD must follow State requirements for retention of criminal justice data.[5]
3. Does not limit data sharing by policy or statute.	SPD's revised policy 16.170 addresses data sharing and states, "Automated License Plate Reader data will only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law."[6]
4. Does not make clear whether and how audits of inquiries to the system can be conducted (see SIR Sections 4.10 and 8.2, for example).	SPD's Policy 16.170 outlines that the Office of Inspector General (OIG) is responsible for conducting periodic audits of the Automated License Plate Reader system.[7]

[4] See SPD Policy 16.170

[5] Washington State's law enforcement agency retention requirements vary by type of record (e.g. case status and type of investigation)

[6] See also additional references in the SIR to SPD Policy 12.050 for public records requests, SPD Policy 12.055 allowing data sharing with authorized criminal justice researchers, and SPD Policy 12.080 pertaining to requests for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies

[7] Per SPD Policy 16.170, The Office of the Inspector General "may audit Department records at any time to ensure compliance with this policy."

5. Does not make clear how and to what degree Patrol and Parking Enforcement Automated License Plate Reader systems are separated, and whether SPD's policies on Automated License Plate Reader apply to the Parking Enforcement Systems	Parking Enforcement's AutoVu data[8] and Patrol's Automated License Plate Reader data have different retainage policies and separate administrators. Parking Enforcement Officers (PEOs) do not have access to stored Automated License Plate Reader data in the Patrol system.[9]
6. Does not include measures to minimize false matches.	This concern is adequately covered in the SIR, including confirmation and verification measures.
7. Does not include systematic tracking to assess how many crimes each year are actually solved using Automated License Plate Reader data.	The Office of Inspector General for Public Safety's Annual Surveillance Usage Review should address usage patterns of this technology.
8. Does not create clear restrictions on who can access the data.	SPD Policy clearly states that only authorized users within the Department can access the data collected by Automated License Plate Reader; all access is logged and auditable.

Recommended Policies. The Impact Assessment recommends that Council ensure that SPD adopt "clear and enforceable policies that ensure, at a minimum, the following:

1. The purposes of Automated License Plate Reader use must be clearly defined, and operation and data collected must be explicitly restricted to those purposes only.
2. Dragnet, suspicionless [sic] use of Automated License Plate Reader must be outlawed.
3. Data collected should be limited to license plate images, and no images of vehicles or occupants should be collected.
4. Data retention should be limited to the time needed to effectuate the purpose defined.
5. Data sharing with third parties must be limited to those held to the same restrictions as agency deploying the system."

Table 2 describes how the SIRs as drafted would address these recommendations. Areas not fully addressed are included in the "Policy Considerations" section.

[8] AutoVu is used for Scofflaw enforcement (i.e. vehicle impoundment due to unpaid parking fines), enforcement of time-restricted parking areas and restricted parking zones, and also for identifying stolen vehicles or vehicles sought in connection with criminal investigation.

[9] Section 1.1 of the Privacy Assessment in the SIR states that Parking Enforcement and Patrol are held to the same rules and policies for use of Automated License Plate Readers.

Table 2. Working Group Recommendations Addressed in the SIR

Working Group Recommendation	Whether/How Addressed in SIR
1. Define the purposes of Automated License Plate Reader use and restrict its operation and data collection use to those purpose.	**Executive Overview.** Operational Policies represent the only allowable uses of the equipment and data collected by this technology. Note: the Executive Overview is not adopted by CB 120004. *See "Policy Considerations"*
2. Outlaw "dragnet, suspicionless [sic]" use of the Automated License Plate Reader	**3.20** The use of Automated License Plate Readers is limited to the "search of specific or partial plate(s) and/or vehicle identifiers as related to: a crime in progress, a search of a specific area as it relates to a crime in-progress, a criminal investigation, a search for a wanted person, or community caretaking functions such as locating an endangered or missing person."
3. Limit data collection to license plate images; prohibit collection of vehicle or occupants' images	**3.20** The use of Automated License Plate Readers is limited to the "search of specific or partial plate(s) and/or vehicle identifiers **4.9** The Automated License Plate Reader will not be used to intentionally capture images in private area or areas where a reasonable expectation of privacy exists, nor shall it be used to harass, intimidate or discriminate against any individual or group.
4 Limit data retention to the time needed to effectuate the defined purpose	**5.1** All Automated License Plate Reader data is deleted after 90 days unless it is related to a criminal investigation and exported in support of that investigation prior to 90 days[10]
5 Limit data sharing with third parties to those held to the same restrictions as the agency deploying the system	**6.3** Law enforcement agencies receiving criminal history information are subject to state and federal data sharing regulations.[11] Once disclosed in response to Public Records Act 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.

[10] This is consistent with LE2010-054 and LE2010-055 of Washington State's Law Enforcement Records Retention Schedule for Violations and Traffic Enforcement.

[11] Federal regulations include 28 CFR Part 20. Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260, and RCW Chapter 10.97.

Policy Consideration

Central Staff has identified the following potential policy consideration relative to the Working Group's key concerns and recommendations:

1. Restrictions on use. SPD's policies do not concisely specify the allowable uses of the Automated License Plate Reader technology. Council may wish to amend the proposed Council Bill to also adopt the Executive Overview of the SIR which identifies specific language as constituting the enforceable policies and procedures applicable to the technology.

2. Parking Enforcement Systems

CB 120004 would approve SPD Parking Enforcement Officers' continued use of and accept the SIR for Genetec's AutoVu Automated License Plate Reader hardware. The SIR states that all rules and policies that govern Patrol's use of Automated License Plate Reader technology are "applicable in the same manner" as they are when it is used by Parking Enforcement. An October 2018 version of the SIR was updated in January 2019 to align with revised SPD policies pertaining to Patrol's use of Automated License Plate Readers. References to the new policies are noted in the updated SIR next to the original policy references.

Parking Enforcement Officers use the AutoVu hardware with the following software and devices, which the SIR describes as "non-surveillance technologies":

- Genetec's Patroller software, the interface and backend server through which retention periods are set (and auditable), user permissions are managed, user activity is tracked and logged, and camera "read" and "hit" data is accessible.
- Samsung devices allow Officers to access the software required to write tickets and enter ticket information.
- Gtechna software prints citations for vehicles found in violation of scofflaw, overtime zone parking, and metered parking.

When this SIR was prepared, eight parking enforcement vehicles carried Automated License Plate Reader equipment, including high definition infrared digital cameras on three vehicles designated for "scofflaw enforcement" – immobilization of vehicles with multiple unpaid parking tickets. All data collected from those cameras is retained in the "BOSS" database[1] for 90 days, unless a record is related to a parking violation or criminal investigation. The other five vehicles are equipped to digitally "chalk" vehicles parked in time-restricted zones, using GPS location and stem-valve comparison technology. All data collected from those five vehicles is deleted from the system at the end of each shift, except for records identified as being related to a parking violation or criminal investigation and exported during the shift it was captured.[2]

Civil Liberties and Potential Disparate Impacts on Historically Marginalized Communities

Departments submitting a SIR are required to complete an adapted version of the Racial Equity Toolkit (RET) to inform the SIR public engagement process and to highlight and mitigate impacts on racial equity from the use of the technology. The RET for SPD's Parking Systems Enforcement identifies the same civil liberties risks as for Automated License Plate Reader technology. These include the risk that, without appropriate policy, license plate data could be used to identify individuals without reasonable suspicion of having committed a crime, or to search for information that is not incidental to any active investigation. It also cites the same potential concern that SPD would over-surveil vulnerable or historically targeted communities, deploying Automated License Plate Readers to diverse neighborhoods more often than to other areas of the City.

[1] Neology Back Office System Software, or "BOSS"

[2] SPD currently has six sedans, two vans and one truck.

In addition to the updated Automated License Plate Reader Polices described above, the SIR describes the following actions by which SPD will ensure that parking enforcement occurs equitably throughout the City: follow policy limiting use of Automated License Plate Reader technology to routine parking enforcement; delete all data collected by parking enforcement vehicles with Automated License Plate Reader technology at the end of the parking enforcement officer's shift; ensure that collected data is used for legitimate law-enforcement purposes; continue to audit the system on a regular basis.

Public Engagement

The Executive accepted public comments on this technology from October 8, 2018 through November 5, 2018 and conducted three public meetings to solicit public comment on this SIR and the SIR for SPD's Parking Enforcement Systems on October 22, 29 and 30, 2018. In addition, the Department of Neighborhoods conducted two focus groups on November 8 and November 20, 2018. Appendix B in the SIR includes a statistical analysis of public comments a (specific to Parking Enforcement Systems) and demographics (including all Group 1 SIR Comments); Appendix E contains comments and survey results received from members of the public, some which expressed support for this technology and others which expressed a wide range of privacy concerns including data retention, equitable enforcement, and surveillance in general; Appendix F contains letters from three organizations concerned about issues including integration with the Patrol's Automated License Plate Reader technology, data access, retention and sharing, and transparency; and Appendix G contains letters submitted from the public expressing concern about surveillance in general and about issues including integration with the Patrol's Automated License Plate Reader technology data and data retention.

Privacy and Civil Liberties Impact Assessment – Parking Enforcement Systems

The Working Group's Impact Assessment states that the same concerns identified about SPD's patrol officers' use of Automated License Plate Readers apply equally to its Impact Assessment of Parking Enforcement Systems. In addition, the Impact Assessment identifies three concerns about the use of SPD's Parking Enforcement Systems technology and recommends that Council adopt four specific policies. The concerns include questions about the allowable use of these systems and the data collected by them, over-collection and over-retention of data, and sharing of data with third parties. The following sections summarize the CTO's Response to the concerns and describe whether and how the SIR as drafted would address the Working Group's recommended policies.

Working Group Concerns and the CTO's Response. Table 3 summarizes CTO's response to each of the Working Group's concerns. The Response concludes that SPD's updated policy, training and limitations from the technologies themselves provide adequate mitigation for the potential privacy and civil liberty concerns raised by the Working Group.

Table 3. CTO Response to Privacy and Civil Liberties Impact Assessment of SPD's Parking Enforcement Systems Technology

Working Group Concern	CTO Response
1. The use of these systems and the data collected by them for purposes other than those intended.	Appropriate policies and technology are in place to restrict data use and access.
2. Over-collection and over-retention of data	SPD must follow State requirements for retention of criminal justice data. Data collected by AutoVu (parking enforcement system) is not retained after the end of the officer's shift.
3. Sharing of data with third parties (such as federal law enforcement agencies)	SPD's revised policy 16.170 addresses data sharing and states, "Automated License Plate Reader data will only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law."

Recommended Policies. The Impact Assessment makes the following recommendations:

- SPD's policy must require that the data collected by Parking Enforcement Automated License Plate Reader systems is not shared with Patrol Automated License Plate Reader systems.
- SPD's policy must require all data-sharing relationships to be disclosed to the public in clear terms, and, as stated above in the Automated License Plate Reader-Patrol Section, SPD's policy must limit sharing of Automated License Plate Reader data to third parties that have a written agreement holding those third parties to the same use, retention, and access rules as SPD, and requiring disclosure of to whom and under what circumstances the data are disclosed.
- SPD's policy must require detailed records of Automated License Plate Reader scans, hits, and revenue generated specifically attributable to those hits, as well as an accounting of how Automated License Plate Reader use varies by neighborhood and demographic.
- SPD's policy must make explicit what photos are taken by the Automated License Plate Reader on Parking Enforcement vehicles, and require the same 48-hour maximum retention period for all photos.

Table 4 describes how the SIR as drafted would address these recommendations. Areas not fully addressed are included in the "Policy Considerations" section.

Table 4. Working Group Recommendations Addressed in the SIR

Working Group Recommendation	Whether/How Addressed in SIR
1. Data collected by Parking Enforcement Automated License Plate Reader systems must not be shared with Patrol Automated License Plate Reader systems.	**2.5** Parking enforcement ALPR data collected by Scofflaw enforcement boot vans is stored with Patrol ALPR data in the Neology Back Office System Software (BOSS). **4.4** Parking enforcement officers upload Automated License Plate Reader data from their shift to the BOSS server prior to shutting down their computer. *See "Policy Considerations"*
2. Disclose all data-sharing relationships to the public and limit data sharing with third parties to those held via written agreement to the same restrictions as SPD	**6.1** This section of the SIR lists all the outside entities with whom parking enforcement data may be shared. **6.3** Law enforcement agencies receiving criminal history information are subject to state and federal regulations.[3] Once disclosed in response to Public Records Act 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.
3. Keep detailed records of Automated License Plate Reader scans, hits, and revenue generated specifically attributable to those hits, as well as an accounting of how Automated License Plate Reader use varies by neighborhood and demographic.	**2.2** This section of the SIR provides the revenue collected from parking citation sin 2016 and 2017. **2.5** Parking enforcement ALPR data collected by Scofflaw enforcement boot vans is stored with Patrol ALPR data in the Neology Back Office System Software (BOSS). **4.10** All activity in the AutoVu system is logged and can be audited.
4. Make explicit what photos are taken by the Automated License Plate Reader on Parking Enforcement vehicles, and require the same 48-hour maximum retention period for all photos	**4.1** Automated License Plate Readers on Parking Enforcement vehicles take a burst of 26 pictures of each parked vehicle, for visual photo comparison when the same vehicle is later examined for time zone violation. **4.9** Automated License Plate Readers will not be used to intentionally capture images in private area or areas where a reasonable expectation of privacy exists, nor shall it be used to harass, intimidate or discriminate against any individual or group. **4.4** Parking enforcement officers upload Automated License Plate Reader data from their shift to the BOSS server prior to shutting down their computer. **4.2** All data collected by the Parking Enforcement sedans is deleted after 90 days unless it is related to a criminal investigation and exported in support of that investigation prior to 90 days[4]

[3] Federal regulations include 28 CFR Part 20. Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260, and RCW Chapter 10.97.

[4] This is consistent with LE2010-054 and LE2010-055 of Washington State's Law Enforcement Records Retention Schedule for Violations and Traffic Enforcement.

Policy Considerations

Central Staff has identified the following potential policy consideration relative to the Working Group's key concerns and recommendations:

1. Restrictions on use. SPD's policies do not concisely specify the allowable uses of the Parking Enforcement Systems technology. Council may wish to amend the proposed Council Bill to also adopt the Executive Overview of the SIR which identifies specific language as constituting the enforceable policies and procedures applicable to the technology.
2. Data Sharing between Patrol and Parking Enforcement. SPD's current policies and practice provide for data sharing between the automated license plate reader systems used during Patrol and Parking Enforcement operations. Council may wish to amend the SIR to restrict such sharing.
3. Parking Enforcement System – Equitable Enforcement. The SIR describes a series of actions that Parking Enforcement Officers will take that will ensure that parking enforcement occurs equitably throughout the City, but the SIR does not describe whether the Parking Enforcement System technologies are being used in such a way as to ensure equitable enforcement. Council may wish to request that the Office of Inspector General review this issue as part of its Annual Surveillance Usage Review.
4. Parking Enforcement System – Genetec Patroller Software. Section 1.1 of the SIR describes Genetec's Patroller software as "non-surveillance" technology. However, this software is used for storing and retaining data once it is captured by the AutoVu hardware, which has been classified as surveillance technology. Section 2.3 of the SIR states that Patroller is used to set retention periods, manage user permissions, track and log user activity and access camera data. Section 4.10 of the SIR describes safeguards for protecting data both in the AutoVu system and in "Parking Enforcement software systems." Council may wish to amend the SIR to include the Patroller software in the definition of the Parking Enforcement Systems surveillance technology.

3. Computer-Aided Dispatch

CB 120004 would approve SPD's continued use of and accept the SIR for software, made by Versaterm, used by SPD's 911 center and patrol officers to respond to 911 calls. The software collects information from 911 callers, informs dispatchers as to patrol unit availability and documents SPD's response to the calls, after which the information is stored in SPD's Records Management System. SPD retains this data for 90 days, unless it is related to an investigation, in which case it is maintained for the retention period applicable to the type of case. Authorized SPD users can extract information for use in legal proceedings and to respond to requests for information.

Discrete pieces of data may be shared with other law enforcement agencies, but all requests for data from Federal Immigration and Customs Enforcement are referred to the Mayor's Office Legal Counsel, per the Mayoral Directive dated February 6, 2018. If a non-emergency call requires police services, officers or dispatchers will enter relevant information manually into the Computer-Aided Dispatch system. SPD's dispatch center transfers calls requiring a fire or medical response that do not also require a police response to the Seattle Fire Alarm Center; those calls are not entered into SPD's Computer-Aided Dispatch system.

Civil Liberties and Potential Disparate Impacts on Historically Marginalized Communities

Departments submitting a SIR are required to complete an adapted version of the Racial Equity Toolkit (RET) to inform the SIR public engagement process and to highlight and mitigate impacts on racial equity from the use of the technology. The RET for the SPD's Computer-Aided Dispatch identifies potential civil liberties impacts from disclosure of personally identifiable information gathered during 911 calls. The SIR states that SPD mitigates the risk of unintentional release of privacy data through data security processes and by requiring state ACCESS certification (A Central Computerized Enforcement Service System) and federal CJIS (Criminal Justice Information Services) certification for all CAD users.

The SIR also identifies data sharing, storage and retention as having the potential to contribute to structural racism, thereby creating a disparate impact on historically targeted communities.[1] The SIR states that SPD mitigates this risk through policies regarding the dissemination of data in connection with criminal prosecutions, the Washington Public Records Act, and other authorized researchers. In addition, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures. The RET does not identify metrics to be used as part of the CTO's annual equity assessments.[2]

[1] Historical community or department practices could produce data in a CAD system that would portray certain communities as higher in crime than in other neighborhoods or elevate the involvement in potential criminal events by certain demographic groups. An approach to storage, retention, and integration of these data that was not cognizant of these possibilities might allow for the continuation of these perceptions, with potential disparate enforcement responses.

[2] SMC 14.18.050B requires that the CTO produce and submit to the City Council a Surveillance Technology Community Equity Impact Assessment and Policy Guidance Report that addresses whether Chapter 14.18 of the SMC is effectively meeting the goals of the Race and Social Justice Initiative, any recommended adjustments to laws and policies to achieve a more equitable outcome, and any new approaches and considerations for the SIRs.

Public Engagement

The Executive accepted public comments on this technology from February 5 – March 5, 2019 and conducted one public meeting for multiple SIRs on February 27, 2019.[3] In addition, the Department of Neighborhoods conducted four focus groups in partnership with organizations serving communities of color and other marginalized communities.[4] The SIR includes all notes from the focus groups (Appendix D); comments pertaining solely to these technologies received from members of the public (Appendix E), department responses to public inquiries (Appendix F); and, letters from organizations or commissions (Appendix G). Of the very few public comments received about this technology, concerns included support for the technology, concerns about security of data, and concern about the distribution of an all-points bulletin known as "BOLO" (be on the lookout) via the system. Letters from organizations expressed concern about the need for limitations on the use of data, data retention and sharing, and about the age of the system.

Privacy and Civil Liberties Impact Assessment – Computer-Aided Dispatch

The Impact Assessment identifies three concerns about the use of SPD's Computer-Aided Dispatch technology and recommends that Council adopt four specific policies. The concerns include the lack of a policy defining the purpose of the technology and limiting its use to that purpose, data retention and access to data. The following sections summarize the CTO's Response to the concerns and describe whether and how the SIR as drafted would address the Working Group's recommended policies

Key Concerns and the CTO's Response. Table 5 summarizes CTO's response to each of the Working Group's concerns. In his response to the Impact Assessment, the City's CTO found that that the SIR provided information specific to each concern.

Table 5. CTO Response to Privacy and Civil Liberties Impact Assessment of SPD's Computer-Aided Dispatch Technology

Working Group Concern	CTO Response
1. No policy defining the purpose of the technology and limiting its use to that purpose	SPD policies and limitations pertaining to the purpose and use of data collected through the CAD system are clearly outlined in the SIR response.
2. Unclear whether and what data is retained within the Computer-Aided Dispatch and Records Management Systems	The specifics about retention of data collected by law enforcement are clearly provided in the SIR.

[3] The February 27, 2019 City Surveillance Technology Fair solicited comments on three Seattle Police Department Technologies: 911 Call Logging Recorder, Computer-Aided Dispatch, and CopLogic; Seattle Fire Department's Computer-Aided Dispatch technology; Seattle City Light's Current Diversion Technologies; and Seattle Department of Transportation's Acyclica travel time measurement technology. The Fair flyer in the SIR erroneously lists the year of the meeting as "2018" instead of "2019."

[4] Appendix D contains notes from these focus group meetings, which were conducted as part of a "World Café" pilot project in collaboration with the Council on American-Islamic Relations, Entre Hermanos, Byrd Barr Place, and Friends of Little Saigon. Notes from Entre Hermanos are in Spanish; Executive staff are reviewing options to translate these notes into English.

3. Unclear which internal and third parties have access to SPD's Computer-Aided Dispatch Data	Details about legal obligations, SPD policy and technology access controls for data access and sharing are provided in the SIR.

Recommended Policies. The Impact Assessment recommends that Council ensure that SPD adopt "clear and enforceable policies that ensure, at a minimum, the following:

1. The purpose of use must be clearly defined as emergency operations, and the operation and data collected by the tool must be explicitly restricted to that purpose only.
2. Data retention within CAD, to the extent there is any, must be limited to the time needed to effectuate the emergency operations purpose defined.
3. Data sharing with third parties, if any, must be limited to those held to the same restrictions.
4. Clear policies must govern operation, and all operators should be trained in those policies."

Table 6 describes how the SIR as drafted would address these recommendations. Areas not fully addressed are included in the "Policy Considerations" section.

Table 6. Working Group Recommendations Addressed in the SIR

Working Group Recommendation	Whether/How Addressed in SIR
1. Define the purpose of Computer-Aided Dispatch (SPD) as emergency operations and restrict its operation and data collected to that purpose.	**Executive Overview.** Operational Policies represent the only allowable uses of the equipment and data collected by this technology. Note: the Executive Overview is not adopted by CB 120003. *See "Policy Considerations"*
2. Limit retention of data within CAD to the time needed to effectuate the emergency operations purpose	SPD must follow State requirements for retention of criminal justice data.
3. Limit data sharing with third parties to those held to the same restrictions as the agency deploying the system	**6.3** Law enforcement agencies receiving criminal history information are subject to state and federal regulations.[5] Once disclosed in response to a Public Records Act 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.
4. Operation of Computer-Aided Dispatch should be governed by clear policies in which all operators have been trained.	**7.2** SPD Dispatchers undergo training on the use of CAD, which includes privacy training. All authorized users of CAD must be CJIS certified and must maintain Washington State ACCESS certification.

[5] Federal regulations include 28 CFR Part 20. Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260, and RCW Chapter 10.97.

Policy Considerations

Central Staff has identified the following potential policy considerations relative to the Working Group's key concerns and recommendations:

1. Restrictions on use. SPD's policies do not concisely specify the allowable uses of Computer-Aided Dispatch and its data. Council may wish to amend the proposed Council Bill to also adopt the Executive Overview of the SIR which identifies specific language as constituting the enforceable policies and procedures applicable to the Computer-Aided Dispatch technology.
2. Annual equity assessment metrics. SPD has not finalized metrics to be used in evaluating the Computer Aided Dispatch Technology as part of the CTO's annual equity assessments. These assessments are intended to play a key role in determining whether the City's surveillance legislation is meeting the goals of the Race and Social Justice Initiative. Council may wish to request a report on the proposed metrics by a date certain and/or Council may wish to defer approval of this SIR, pending completion of these metrics.

4. CopLogic

CB 120004 would approve SPD's continued use of and accept the SIR for CopLogic, a crime reporting software tool owned by LexisNexis. The software has two applications: 1) individuals may report a low-level crime[1] in which no known or describable suspect is available, and for which individuals may need proof of police reporting (i.e., for insurance purposes), and 2) businesses that participate in SPD's Retail Theft Program may enter information about retail theft on their property in which a suspect is known and suspect information is available.[2] Reports from individuals are assigned a general offense number for their records and for insurance purposes.

Businesses complete an online Security Incident Report, which may include copies of identification if security personnel have detained the suspect. The business issues a written trespass warning to the suspect, photographs the suspect and then may release the individual or turn them over to the police. An SPD detective reviews the Security Incident Report and submits the reviewed case to the City Attorney's Office to be reviewed for charges. Once either type of report has been screened and accepted by SPD personnel, it is transferred into SPD's Records Management System.

The SIR includes historical data on CopLogic's effectiveness from 2012, with 2018 figures showing a reduction of 20,356 police hours and savings over $1 million by eliminating the need for a patrol officer to respond in person to these incidents.

Civil Liberties and Potential Disparate Impacts on Historically Marginalized Communities

Departments submitting a SIR are required to complete an adapted version of the Racial Equity Toolkit (RET) to inform the SIR public engagement process and to highlight and mitigate impacts on racial equity from the use of the technology. The RET for the CopLogic technology identifies two potential civil liberties risks: 1) that information from the system could be disseminated intentionally or unintentionally in ways that could negatively impact peoples' civil liberties; and 2) the risk that racial or ethnicity-based biased information may be entered into the system. The SIR states that SPD mitigates those risks by screening information entered into the system[3] and by virtue of the fact that SPD employees are subject to multiple department policies pertaining to computer and records access, dissemination of data and policies prohibiting bias-based policing.[4] The SIR also identifies data sharing, storage and retention as having the potential to contribute to structural racism, thereby creating a disparate impact on historically

[1] The crime must be within one of these categories of crime: a. Property crimes including property destruction, graffiti, car break ins, theft of auto accessories, theft, shoplifting; or b. Drug activity, harassing phone calls, credit card fraud, wage theft, identity theft, or lost property

[2] SPD's Retail Theft webpage reports that approximately 120 stores participate in this program.

[3] Screeners do not edit the information received through CopLogic, other than accidentally incorrect information that the reviewing officer or reporting party identifies.

[4] All SPD employee 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.

targeted communities. The SIR states that SPD mitigates this risk through policies regarding the dissemination of data in connection with criminal prosecutions, the Washington Public Records Act, and other authorized researchers. The RET also reports that SPD had not yet finalized the metrics to be used as part of the CTO's annual equity assessments.[5]

Public Engagement

The Executive accepted public comments on this technology from February 5 – March 5, 2019 and conducted one public meeting for multiple SIRs on February 27, 2019.[6] In addition, the Department of Neighborhoods conducted four focus groups in partnership with four organizations serving communities of color and other marginalized communities.[7] The SIR includes all notes from the focus groups (Appendix D); comments pertaining solely to these technologies received from members of the public (Appendix E), department responses to public inquiries (Appendix F); and, letters from organizations or commissions (Appendix G). Comments included support for and concerns about the technologies. Several of the supportive comments included requests for the technology to be available in languages other than English. Concerns included uneven access to the programs for those without computers or English fluency, the potential for racial bias in both kinds of reporting and for inaccurate reports, unfair treatment of individuals suspected of shoplifting, the potential for LexisNexis to use inaccurate information for crime mapping, and questions about data collection, retention and sharing.

Privacy and Civil Liberties Impact Assessment – CopLogic

The Impact Assessment identifies three concerns about the use of SPD's CopLogic technology and recommends that Council adopt specific policies and contract provisions. The concerns include data retention, civil liberty impacts of the retail theft program, and third-party data sharing. The following sections summarize the CTO's Response to the concerns and describe whether and how the SIR as drafted would address the Working Group's recommended policies.

In his response to the Privacy and Civil Liberties Impact Assessment, the City's CTO found that that SPD's policy, training and limitations from the technology itself outlined in the SIR provide

[5] SMC 14.18.050B requires that the CTO produce and submit to the City Council a Surveillance Technology Community Equity Impact Assessment and Policy Guidance Report that addresses whether Chapter 14.18 of the SMC is effectively meeting the goals of the Race and Social Justice Initiative, any recommended adjustments to laws and policies to achieve a more equitable outcome, and any new approaches and considerations for the SIRs.
[6] The February 27, 2019 City Surveillance Technology Fair solicited comments on three Seattle Police Department Technologies: 911 Call Logging Recorder, Computer-Aided Dispatch, and CopLogic; Seattle Fire Department's Computer-Aided Dispatch technology; Seattle City Light's Current Diversion Technologies; and Seattle Department of Transportation's Acyclica travel time measurement technology. The Fair flyer in the SIR erroneously lists the year of the meeting as "2018" instead of "2019."
[7] Appendix D contains notes from these focus group meetings, which were conducted as part of a "World Café" pilot project in collaboration with the Council on American-Islamic Relations, Entre Hermanos, Byrd Barr Place, and Friends of Little Saigon. Notes from Entre Hermanos are in Spanish; Executive staff are reviewing options to translate these notes into English.

adequate mitigation for the potential privacy and civil liberty concerns raised by the Working Group. Table 7 summarizes CTO's response to each of the Working Group's concerns.

Table 7. CTO Response to Privacy and Civil Liberties Impact Assessment of SPD's CopLogic Technology

Working Group Concern	CTO Response
1. Lack of specific data retention policies	SPD has adequately addressed the policies and practices in place regarding data retention for the information collected through CopLogic.
2. Civil liberties concerns about the retail track	Validation of retail owner reports through the investigative process mitigates the potential for bias or civil liberties infringement through raw information provided by residents into CopLogic
3. Lack of prohibition about LexisNexis data retention and third-party sharing	Data use policies and limitations to data access is detailed in the SIR

Recommended Policies. The Impact Assessment recommends that Council ensure that SPD adopt "clear and enforceable policies that ensure, at a minimum, the following:

1. CopLogic data may be used only for purposes of allowing community members to file police reports or investigating and, as appropriate, prosecuting crimes.
2. The contract between the City of Seattle and LexisNexis must include the following minimum provisions:
    a. LexisNexis may not use CopLogic data for any purpose other than providing the CopLogic tool to the City of Seattle and interfacing it with Mark43[8].
    b. LexisNexis must immediately delete all CopLogic data after that data has been transferred to SPD's records management system (RMS). LexisNexis must delete all CopLogic data within 30 days of its creation regardless of whether such a transfer has taken place.
    c. LexisNexis must not share CopLogic data with any third party.
    d. LexisNexis and any third party that has access to CopLogic data must be held to the same purpose and use restrictions as SPD.
3. The retail track of CopLogic must be discontinued. Retailers should still be allowed to access and use CopLogic to provide information as any other member of the public would."

Table 8 describes how the SIR as drafted would address these recommendations. Areas not fully addressed are included in the "Policy Considerations" section.

[8] "Mark43" appears to refer to SPD's records management system.

Table 8. Working Group Recommendations Addressed in the SIR

Working Group Recommendation	Whether/How Addressed in SIR
1. CopLogic data may be used only for purposes of allowing community members to file police reports or investigating and, as appropriate, prosecuting crimes.	The SIR allows for use by individuals to report a low-level crime and by retailers to report retail theft. *See "Policy Considerations"*
2. Add restrictions pertaining to the purpose and use, retention and sharing of CopLogic data to the City's contract with LexisNexis; data sharing with third parties must be held to the same purpose and use restrictions as SPD.	**4.8** There are no data sharing agreements between SPD and any other entities for CopLogic data. The contract between the City and LexisNexis provides that LexisNexis may only "use, transmit, distribute, modify, reproduce, display, and store the City Data solely for the purposes of (i) providing the Services as contemplated in [its contract with the City]; and (ii) enforcing its rights under [the contract]." *See "Policy Considerations"*
3. Discontinue the "retail track" of CopLogic.	The SIR allows for use by individuals to report a low-level crime and by retailers to report retail theft. *See "Policy Considerations"*

Policy Considerations

Central Staff has identified the following potential policy considerations relative to the Working Group's key concerns and recommendations:

1. Discontinue retail theft reporting component of CopLogic. If Council wishes to discontinue the retail theft reporting component of CopLogic, the SIR and Executive Overview would need to be amended.
2. Restrictions on use. SPD's policies do not concisely specify the allowable uses of CopLogic and its data and currently allow for retailers to report retail theft. If Council wishes to discontinue the retail theft reporting component of CopLogic, the SIR and Executive Overview would need to be amended. Council could then adopt an amended Executive Overview of the SIR which identifies specific language as constituting the enforceable policies and procedures applicable to a more restricted use of the CopLogic technology.
3. Lexis-Nexis Contract Provisions. The SIR does not have an explicit policy that third parties with whom SPD shares data must comply with the same privacy provisions as SPD. Council may wish to direct SPD to incorporate this requirement and other restrictions pertaining to the purpose and use, retention and sharing of CopLogic data requirement into its written agreements, where feasible.
4. Annual equity assessment metrics. SPD has not finalized metrics to be used in evaluating the CopLogic Technology as part of the CTO's annual equity assessments. These assessments are intended to play a key role in determining whether the City's surveillance legislation is meeting the goals of the Race and Social Justice Initiative. Council may wish to request a report on the proposed metrics by a date certain and/or Council may wish to defer approval of this SIR, pending completion of these metrics.

5. 911 Logging Recorder

CB 120004 would approve SPD's continued use of and accept the SIR for software that records all telephone calls to SPD's 911 communications center and to the police non-emergency phone line, as well as police radio traffic. Authorized personnel also use this technology to retrieve recordings for law enforcement or public disclosure purposes. The audio recordings are routinely used in criminal prosecutions and within the 911 Center for training and quality control purposes and some information from the recordings may be stored for future reference in emergency situations. Use of the technology for any other purpose is subject to SPD disciplinary action. SPD Policy requires deletion of audio recordings not requested within 90 days of their capture.[1] SPD downloads and maintains recordings requested for law enforcement and public disclosure for the retention period related to the incident type.

Civil Liberties and Potential Disparate Impacts on Historically Marginalized Communities

Departments submitting a SIR are required to complete an adapted version of the Racial Equity Toolkit (RET) to inform the SIR public engagement process and to highlight and mitigate impacts on racial equity from the use of the technology. The RET for the 911 Logging Recorder identifies potential civil liberties impacts from disclosure of personally identifiable information gathered during 911 calls. The SIR states that SPD mitigates the risk of unintentional release of privacy data through data security processes and by requiring state ACCESS certification (A Central Computerized Enforcement Service System) and federal CJIS (Criminal Justice Information Services) certification for all CAD users.

The SIR also identifies data sharing, storage and retention as having the potential to contribute to structural racism, thereby creating a disparate impact on historically targeted communities.[2] The SIR states that SPD mitigates this risk through policies regarding the dissemination of data in connection with criminal prosecutions, the Washington Public Records Act, and other authorized researchers. In addition, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures. The RET reports that SPD had not yet finalized the metrics to be used as part of the CTO's annual equity assessments.[3]

[1] LE06-01-03 Rev 1 in Washington State Law Enforcement Records Retention Schedule establishes a 90-day retention period for recordings of radio transmissions between law enforcement and dispatch staff regarding requests for resources, status changes and/or incident-related activity. This also matches the retention requirements for Emergency Communications (911) Records Retention.

[2] Historical community or department practices could – could produce data in a CAD system that would portray certain communities as higher in crime than in other neighborhoods or elevate the involvement in potential criminal events by certain demographic groups. An approach to storage, retention, and integration of these data that was not cognizant of these possibilities might allow for the continuation of these perceptions, with potential disparate enforcement responses.

[3] SMC 14.18.050B requires that the CTO produce and submit to the City Council a Surveillance Technology Community Equity Impact Assessment and Policy Guidance Report that addresses whether Chapter 14.18 of the SMC is effectively meeting the goals of the Race and Social Justice Initiative, any recommended adjustments to laws and policies to achieve a more equitable outcome, and any new approaches and considerations for the SIRs.

Public Engagement

The Executive accepted public comments on this technology from February 5 – March 5, 2019 and conducted one public meeting for multiple SIRs on February 27, 2019.[4] In addition, the Department of Neighborhoods conducted four focus groups in partnership with four organizations serving communities of color and other marginalized communities.[5] The SIR includes all notes from the focus groups (Appendix D); comments pertaining solely to these technologies received from members of the public (Appendix E), and letters from organizations or commissions (Appendix G). The Executive received very few comments on this technology. Two of the three public comments specific to the 911 Logging Recorder were supportive of the technology, the third raised several technical issues, including challenges that could be presented by Voice over Internet protocols. Other concerns included data use, retention and sharing.

Privacy and Civil Liberties Impact Assessment – 911 Logging Recorder

The Impact Assessment identifies three concerns about the use of SPD's 911 Logging Recorder and recommends that Council adopt four specific policies. The concerns include restrictions on the purpose and use of the technology, as well as data retention and data sharing. The following sections summarize the CTO's Response to the concerns and describe whether and how the SIR as drafted would address the Working Group's recommended policies.

In his response to the Privacy and Civil Liberties Impact Assessment, the City's CTO found that that SPD's policy, training and limitations from the technology itself outlined in the SIR provide adequate mitigation for the potential privacy and civil liberty concerns raised by the Working Group. Table 9 summarizes CTO's response to each of the Working Group's concerns.

Table 9. CTO Response to Privacy and Civil Liberties Impact Assessment of SPD's 911 Logging Recorder Technology

Working Group Concern	CTO Response
1. Lack of clear policy defining the purpose and allowable uses of the Logging Recorder Data.	The responses in the appropriate sections of the SIR provide clear and detailed information about the laws and policies regarding the use and access to this system.
2. Justification for the 90-day data retention period for Logging Recorder data.	This period of time provides adequate time for any investigation, review, audit or litigation that may occur regarding the recordings.

[4] The February 27, 2019 City Surveillance Technology Fair solicited comments on three Seattle Police Department Technologies: 911 Call Logging Recorder, Computer-Aided Dispatch, and CopLogic; Seattle Fire Department's Computer-Aided Dispatch technology; Seattle City Light's Current Diversion Technologies; and Seattle Department of Transportation's Acyclica travel time measurement technology. The Fair flyer in the SIR erroneously lists the year of the meeting as "2018" instead of "2019."

[5] Appendix D contains notes from these focus group meetings, which were conducted as part of a "World Café" pilot project in collaboration with the Council on American-Islamic Relations, Entre Hermanos, Byrd Barr Place, and Friends of Little Saigon. Notes from Entre Hermanos are in Spanish; Executive staff are reviewing options to translate these notes into English.

3. Lack of clarity about third-party data sharing content and purpose or justification.	SPD provides clear and adequate details about third party agencies with whom the 911 logging recording data is shared and for what purposes. Specification and compliance to the agreements between departments and agencies are provided in the SIR, including information about the Washington Public Records Act and possible redaction or exemptions.

Recommended Policies. The Impact Assessment recommends that Council ensure that SPD adopt "clear and enforceable policies that ensure, at a minimum, the following:

1. The purpose and allowable uses of the Logging Recorder data must be clearly defined, and both SPD and NICE (the vendor of the technology) must be restricted to those uses.
2. NICE must delete all Logging Recorder data after seven days.
3. There must be a clear designation of what data collected by the Logging Recorder is shared with third parties and for what purposes.
4. NICE or any other third party that has access to Logging Recorder data must be held to the same restrictions as SPD, including industry best practice security standards."

Table 10 describes how the SIR as drafted would address these recommendations. Areas not fully addressed are included in the "Policy Considerations" section.

Table 10. Working Group Recommendations Addressed in the SIR

Working Group Recommendation	Whether/How Addressed in SIR
1. Purpose and use of the Logging Recorder data must be defined and both SPD and NICE (the vendor) must be restricted to those uses.	**Executive Overview.** Operational Policies represent the only allowable uses of the equipment and data collected by this technology. Note: the Executive Overview is not adopted by CB 120004. *See "Policy Considerations"*
2. NICE (the vendor) must delete all Logging Recorder data after seven days	**4.2** 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.
3. Clearly designate third-party data sharing and for what purposes	**6.1** Identifies data sharing with other agencies, entities or individuals within legal guidelines or as required by law.
4. NICE or any other third party that has access to Logging Recorder data must be held to the same restrictions as SPD, including industry best practice security standards	**6.1** 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. *See "Policy Considerations"*

Policy Considerations

Central Staff has identified the following potential policy considerations relative to the Working Group's key concerns and recommendations:

1. Restrictions on use - SPD. SPD's policies do not concisely specify the allowable uses of the Automated License Plate Reader technology. Council may wish to amend the proposed Council Bill to also adopt the Executive Overview of the SIR which identifies specific language as constituting the enforceable policies and procedures applicable to the technology.
2. Restrictions on use – NICE. The SIR does not have an explicit policy that third parties with whom SPD shares data must comply with the same privacy provisions as SPD. Council may wish to direct SPD to incorporate this requirement into its contract with NICE or other third parties who have access to Logging Recorder data, where feasible.
3. Annual Equity Assessment Metrics. SPD has not finalized metrics to be used in evaluating the 911 Logging Recorder Technology as part of the CTO's annual equity assessments. These assessments are intended to play a key role in determining whether the City's surveillance legislation is meeting the goals of the Race and Social Justice Initiative. Council may wish to request a report on the proposed metrics by a date certain and/or Council may wish to defer approval of this SIR, pending completion of these metrics.

Attachments:

1. Background Summary and Surveillance Impact Report Process

cc: Dan Eder, Interim Director
Aly Pennucci, Budget and Policy Manager

Attachment 1 - Background Summary and Surveillance Impact Report Process

Recent Legislative History

Ordinance 125376, passed by Council on July 31, 2017, required City of Seattle departments intending to acquire surveillance technology to obtain advance Council approval, by ordinance, of the acquisition and of a surveillance impact report (SIR).[1] Departments must also submit a SIR for surveillance technology in use when Ordinance 125376 was adopted (referred to in the ordinance as "retroactive technologies"). The Executive originally included 28 "retroactive technologies," on its November 30, 2017 Master List but revised that list to 26 in December 2019. The Council has approved two SIRs and twice extended the initial March 3, 2020 deadline for completion of SIRs for all 26 technologies: first by six months to accommodate extended deliberation of the first two SIRS; and then by a second six months due to COVID-related delays. Either the Chief Technology Officer or the Council may determine whether a specific technology is "surveillance technology" and thus subject to the requirements of SMC 14.18. Each SIR must describe protocols for a "use and data management policy" as follows:

- How and when the surveillance technology will be deployed or used and by whom, including specific rules of use
- How surveillance data will be securely stored
- How surveillance data will be retained and deleted
- How surveillance data will be accessed
- Whether a department intends to share access to the technology or data with any other entity
- How the department will ensure that personnel who operate the technology and/or access its data can ensure compliance with the use and data management policy
- Any community engagement events and plans
- How the potential impact of the surveillance on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities have been taken into account; and a mitigation plan
- The fiscal impact of the surveillance technology

Community Surveillance Working Group

On October 5, 2018, Council passed Ordinance 125679, amending SMC 14.18, creating a "community surveillance working group" charged with creating a Privacy and Civil Liberties Impact Assessment for each SIR.[2] At least five of the seven members of the Working Group

[1] As codified in SMC 14.18.030, Ordinance 125376 identified a number of exemptions and exceptions to the required Council approval, including information voluntarily provided, body-worn cameras and cameras installed in or on a police vehicle, cameras that record traffic violations, security cameras and technology that monitors City employees at work.

[2] Ordinance 125679 also established a March 31, 2020 deadline for submitting SIRs on technologies already in use (referred to as "retroactive technologies") when Ordinance 125376 was passed, with provision to request a six-month extension.

must represent groups that have historically been subject to disproportionate surveillance, including Seattle's diverse communities of color, immigrant communities, religious minorities, and groups concerned with privacy and protest.[3] Each Privacy and Civil Liberties Impact Assessment must describe the potential impact of the surveillance technology on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities and will be included in the SIR. Prior to submittal of a SIR to Council, the Chief Technology Officer may provide a written statement that addresses privacy rights, civil liberty or other concerns in the Working Group's impact assessment.

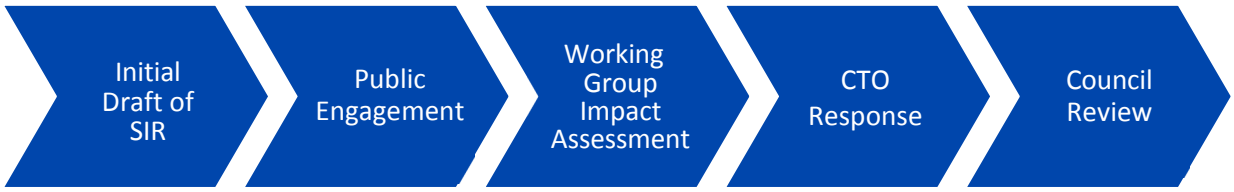
Executive Overviews

In May 2019, members of the Governance, Equity, and Technology Committee requested that IT staff prepare a summary section for each of the two lengthy SIR documents under review at that time. The Committee then accepted the resultant "Condensed Surveillance Impact Reports (CSIRs) together with the complete SIRs. The Executive has continued this practice with subsequent SIRs but has renamed the documents "Executive Overviews." The Operational Policy Statements in the Executive Overview represent the only allowable uses of the subject technology.

SIR Process

Chart 1 is a visual of the SIR process from inception to Council Review:

Chart 1. Surveillance Impact Report (SIR) Process



Department drafts SIR about technology use, privacy, and data security.	Draft SIR made public. One or more public meetings scheduled to solicit feedback.	Working Group reviews SIR; creates Impact Assessment, documenting privacy and civil liberty concerns.	City's Chief Technology Officer addresses any Working Group concerns.	Council reviews Executive's proposed ordinance reflecting the SIR, authorizing the use of existing or new technology.

[3] The Mayor appoints four members and Council appoints three members.