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 120003 - Authorizing approval of uses and accepting the surveillance impact report for the Seattle Fire Department's use of Computer Aided Dispatch[1]

On Wednesday, March 3, 2021 the Transportation and Utilities Committee will discuss Council Bill 120003. The proposed bill is intended to meet the requirements of Seattle Municipal Code Chapter 14.18, Acquisition and Use of Surveillance Technologies.[2] (Attachment 1 to this memo summarizes these requirements and process by which the Executive develops the required Surveillance Impact Reports.) The proposed bill would approve the Seattle Fire Department's (SFD's) continued use of existing Computer-Aided Dispatch technology and accept the Surveillance Impact Report (SIR) and an Executive Overview for this technology. 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 describes each technology and summarizes both the potential civil liberties and potential disparate impacts and the public engagement processes for each, as reported in the SIRs. It also summarizes key concerns and recommendations from the Working Group's Impact Assessment and the CTO's Response. Finally, the memo identifies several policy considerations for possible Council action.

SFD Computer-Aided Dispatch

Council passage of CB 120003 would approve the SFD's continued use of and accept SIRs and an Executive Overview for SFD's Computer-Aided Dispatch technology that supports personnel who dispatch Fire and Emergency Medical Services units in emergency situations. The Executive Overview summarizes the operational policy statements which represent the only allowable uses of the equipment and data collected by the Computer-Aided Dispatch technology. The software advises dispatchers as to the type of unit or units to send in response to 911 emergency and non-emergency calls for fire or medical aid. It determines the type of recommended unit based on the reported problem and location of the caller. The software manufacturer, TriTech, merged in 2018 with two other software companies into one entity called CentralSquare.[3]

---

[1] This memo updates the February 25, 2021 memo on the same subject to reflect that this Council Bill would accept both SIR and the Executive Overview for the Seattle Fire Department's Computer-Aided Dispatch technology and removing related policy considerations.

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

[3] Superion, TriTech Software Systems and its subsidiary, Zuercher Technologies, and Aptean merged into one entity named CentralSquare. The SIR has since been updated to reflect the merger of Tri-Tech with other entities and to make technical corrections to internal references.

<u>Civil Liberties and Potential Disparate Impacts on Historically Marginalized Communities</u>

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 SFD's Computer-Aided Dispatch identifies disclosure of personally identifiable information gathered during 911 calls as a potential civil liberties impact. Such a disclosure could occur in response to a public information request or to a request from an external agency. SFD notes that, while medical information can be redacted from public disclosure, names, phone numbers and addresses are not exempt. SFD works to mitigate this impact by working with requesters to voluntarily redact personal information before disclosure and may provide notice to potentially affected individuals to allow them opportunity to enjoin the release of records via a court order.

The RET also notes that sensitive information on individuals and locations obtained during 911 calls could potentially be used by law enforcement to target members of historically marginalized communities and to track the location and history of requests for services for specific locations and individuals. SFD works to mitigate this risk by providing information to law enforcement officials only if they are conducting an active investigation, as confirmed by SFD's Public Disclosure Officer and recorded for auditing purposes. SFD also uses a quality assurance manager to check data for accuracy and compliance with departmental policies and procedures related to dispatching. The RET does not identify metrics to be used as part of the CTO's annual equity assessments.[4]

<u>Public Engagement</u>

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.[5] In addition, the Department of Neighborhoods conducted four focus group meetings in partnership with four organizations serving communities of color and other marginalized communities.[6] The SIR includes all notes from the focus groups (Appendix D); comments pertaining solely to this technology received from members of the public (Appendix E), and letters from organizations or commissions (Appendix G). The few comments reported about this technology addressed data access and retention, data sharing and transparency.

---

[4] [SMC 14.18.050B](#) requires that the Chief Technology Officer 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.

[5] The February 27, 2019 City Surveillance Technology Fair solicited comments on SFD's Computer-Aided Dispatch technology, as well as Seattle City Light's Current Diversion Technologies, Seattle Department of Transportation's Acyclica travel time measurement technology, and three Seattle Police Department Technologies: 911 Call Logging Recorder, Computer-Aided Dispatch, and CopLogic.

[6] Appendix D contains notes from these 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.

Privacy and Civil Liberties Impact Assessment

The Impact Assessment identifies four "key concerns" about the use of SFD's Computer-Aided Dispatch technology and recommends that Council adopt four specific policies. The "key concerns" include questions about data accessibility, retention and sharing. Tables 1 and 2 below summarize the CTO's Response to the "key 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 1 summarizes CTO's response to each of the Working Group's "Key Concerns." The Response concludes that SFD's 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 1. CTO Response to Privacy and Civil Liberties Impact Assessment of SFD's Computer-Aided Dispatch Technology

Working Group Key Concern	CTO Response
1. No limits on data retention.	Data is retained for the life of the system. All records are kept in accordance with state retention requirements. Two positions in SFD are responsible for ensuring compliance with data retention requirements.
2. Lack of clarity on what data is accessible to the vendor.	Vendor may collect and store data for aggregate reporting services but is prohibited from disclosing Protected Health Information unless permitted by law and may not identify the Customer without Customer's consent.
3. No clear limits on and terms of third-party data sharing.	Role-based requirements restrict access to required services or support the technology. American Medical Response and the City have a Memorandum of Agreement.
4. Lack of clarity on whether original contracts and privacy policies have remained unchanged as a result of the CentralSquare merger.	The privacy and contractual provisions remain unchanged. SFD's Computer-Aided Dispatch data is not shared with the vendor or any of the other customers they have acquired. This SIR was drafted prior to the CentralSquare merger and does not reference this change. (The SIR has since been updated to recognize this change.)

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

1. The purpose of use of Computer-Aided Dispatch (SFD) must be clearly defined as emergency operations, and its operation and data collected must be explicitly restricted to that purpose only.

2. Data retention must be limited to the time needed to effectuate the purpose defined (i.e., Computer-Aided Dispatch data that is no longer needed must be promptly deleted)—in other words, the current indefinite retention policy should be justified or ended.

3. Data sharing with third parties, if any, must be limited to those held to the same restrictions as SFD, and all partnerships and data flows between SFD and third parties must be explicitly disclosed and protected by written agreements.

4. Clear policies must govern operation of Computer-Aided Dispatch, and all operators should be trained in those policies."

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

Table 2. Working Group Recommendations Addressed in the SIR

Working Group Recommendation	Whether/How Addressed in SIR
1. Define the purpose of Computer-Aided Dispatch (SFD) 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.
2. Justify or end the current indefinite data retention policy.	**5.2** All records are kept in accordance with state retention requirements, but data is retained for the life of the system (beyond state retention requirements). *See "Policy Considerations" below.*
3. Data-sharing with third parties must be disclosed, protected by written agreements, and limited to those who meet the same restrictions as SFD	**6.1.** SFD has written agreements with several third parties (American Medical Response, King County EMS, ESO Solutions (vendor for electronic healthcare records). Non-disclosure agreements are required for sharing with "other partners" and SPD must request data through a Public Disclosure Request. The SIR does not identify a policy requiring that its partners are bound by the same restrictions as SFD.
	7.4 states that SPD must comply with Criminal Justice Information Services (CJIS) requirements for investigative data collection, and medical partners must comply with the Health Care Information Access and Disclosure Law. *See "Policy Considerations" below.*
4. Operation of Computer-Aided Dispatch should be governed by clear policies in which all operators have been trained.	**3.1** Only specially trained members of the Fire Alarm Center can input information into CAD.
	7.2 Other department personnel receive yearly training on privacy and security awareness

Policy Considerations

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

1. Data retention. SFD's practice of retaining Computer-Aided Dispatch data for the life of the system exceeds minimum requirements in State law (six years for fire incident reports and three years for Computer-Aided Dispatch Backup Data/Tapes).[7] Council may wish to consider establishing a limit as to the period for which SFD retains Computer-Aided Dispatch data not required for any legal or fire safety investigation.

2. Third-party data sharing. The SIR does not have an explicit policy that third parties with whom SFD shares data must comply with the same privacy provisions as SFD. Council may wish to direct SFD to incorporate this requirement into its written agreements, where feasible.

3. Annual equity assessment metrics. SFD has not yet 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.

Committee Action

Options for Council action are as follows:

1. Pass CB 120003 as transmitted;

2. Request Central Staff to prepare amendments to the Council Bill and/or to the SIR to address additional concerns or issues; or

3. Take no action.

Attachment:

1. Background Summary and Surveillance Impact Report Process

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

---

[7] https://www.sos.wa.gov/archives/recordsmanagement/managing-fire-and-emergency-medical-service-records.aspx, FM53-04-14 Rev. 1; and EM50-20-03 Rev. 0

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.
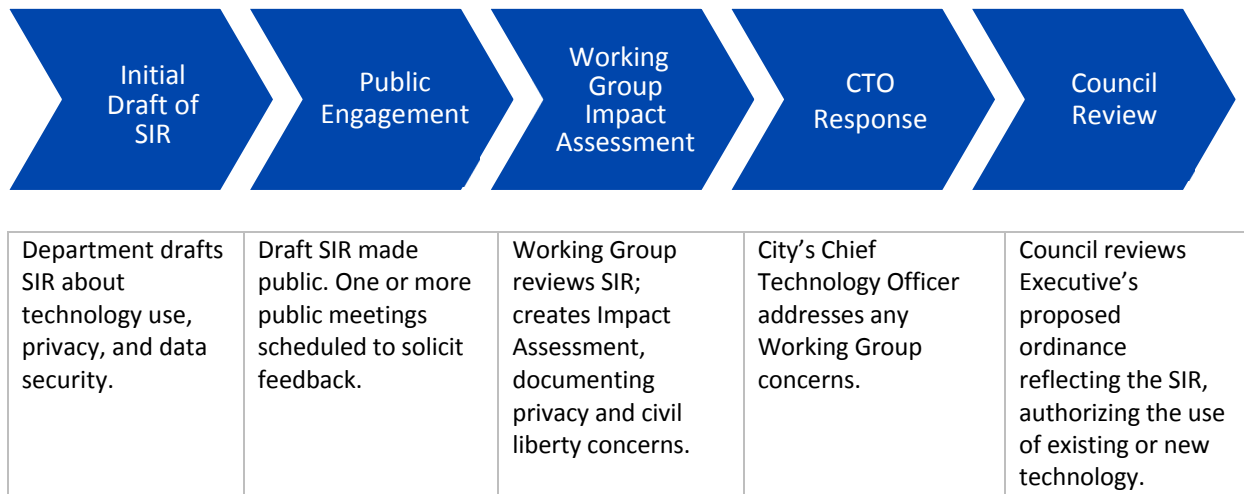
Executive Overviews

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

Initial Draft of SIR	Public Engagement	Working Group Impact Assessment	CTO Response	Council Review
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.