

February 6, 2023

MEMORANDUM

То:	Economic Development, Technology and City Light Committee		
From:	Lise Kaye, Analyst		
Subject:	Council Bill 120503 - Authorizing approval of uses and accepting the surveillance		
	impact report for the Seattle Police Department's use of Remotely Operated		
	Vehicles		

On February 8, 2023, the Economic Development, Technology and City Light Committee will discuss <u>Council Bill (CB) 120503</u>. This CB would approve the Seattle Police Department's (SPD's) continued use of Remotely Operated Vehicles and accept the Surveillance Impact Report (SIR) and an Executive Overview for these technologies.

The bill is intended to meet the requirements of <u>Seattle Municipal Code Chapter 14.18</u>, Acquisition and Use of Surveillance Technologies, which requires City of Seattle departments intending to acquire surveillance technology to obtain advance Council approval of that acquisition and of a surveillance impact report (SIR).¹ Departments must also submit a SIR for surveillance technology in use when <u>Ordinance 125376</u> was adopted in 2017 (referred to in the ordinance as "retroactive technologies"), but failure to approve an ordinance for a retroactive technology does not require SPD to discontinue its use. Councilmembers may choose to amend the ordinance to request additional information or to request that SPD develop new and/or revised operational policies, which, if implemented, could restrict or modify the application of certain technologies.

This memorandum describes SPD's use of Remotely Operated Vehicles, summarizes recommendations from the Community Surveillance Working Group, describes whether and how each recommendation is addressed in the SIR and/or by current law, and summarizes responses by the Chief Technology Officer (CTO) and/or SPD. Finally, the memorandum identifies policy issues for Council consideration.

Remotely Operated Vehicles

SPD's Special Weapons and Tactics (SWAT), Arson/Bomb, and Harbor units use unarmed Remotely Operated Vehicles to access areas that are potentially dangerous for personnel to enter. The SWAT and Arson/Bomb units' Remotely Operated Vehicles have wheels and the Harbor unit's are submersible. All SPD Remotely Operated Vehicles are controlled by SPD employees operating handheld controllers from a safe position nearby. Some Remotely Operated Vehicles have a remotely controlled arm capable of performing simple tasks.

¹ The Executive Overview summarizes SPD's allowable uses of Remotely Operated Vehicles. See also the <u>memorandum</u> summarizing process for developing a Surveillance Impact Report (SIR), consistent with <u>Ordinances 125376</u> and <u>125679</u> and <u>Ordinance 108333</u>, Seattle's "Intelligence Ordinance," adopted in 1979 and amended in 1982 via adoption of <u>Ordinance 100572</u>.

SPD reports that the department mitigates potential civil liberties risks, including the risk of unlawful surveillance and the risks of racial or ethnicity-based bias from the use of these systems and associated data sharing, storage and retention through its warrant parameters, evidence procedures, and anti-bias policies. The Racial Equity Toolkit does not identify metrics to be used as part of the CTO's required annual equity assessments.

Surveillance Working Group Recommendations and CTO Response

The Community Surveillance Working Group's Impact Assessment for Remotely Operated Vehicles makes 11 recommendations to Council. The CTO's response finds that the "policy, training and technology limitations enacted by SPD provide adequate mitigation for the potential privacy and civil liberties concerns raised by the Working Group about the use of this operational technology." The CTO's response does not specifically address the Working Group's recommendations, but it identifies relevant citations from the SIR for each of the "key concerns" raised by the Working Group.

Table 1 summarizes which recommendations have been addressed in the SIR and/or are a matter of state law, and which would require a revised SPD policy and/or procedure. Attachment 1 provides additional detail on whether the SIR as drafted or current law addresses the Working Group's recommendations as well as relevant responses from the CTO and/or SPD.

Addressed in SIR or State Law	SWG Recommendation(s) – Abbreviated
Would require revised SPD policy and/or procedure and	#3. Prohibit SPD from using cell phones to record the livestream on the Remotely Operated Vehicle display
updated SIR	#6. Immediately delete any data collected via Remotely Operated Vehicles not needed for an investigation
	#7. Require that data collected via Remotely Operated Vehicles never leave SPD-owned equipment
	#8. Make equipment information publicly available, including deployment data, number of people with access and contract documentation
	#9. Make information available monthly about each Remotely Operated Vehicle's use and why its data was shared
Would be inconsistent with state law	#2. Require a warrant to use Remotely Operated Vehicles to surveil any members of the public
See citations in Attachment A	#4. Define incident types and usage
	#5. Provide strong access controls
	#10. Provide adequate and standardized training, including a privacy component
	#11. Maintain audit log and produce annual audit report
This is not described in the SIR as an authorized use and a change would require Council	#1. Prohibit use of Remotely Operated Vehicles to deploy weapons.
approval of an updated SIR	

Table 1. Surveillance Working Group (SWG) Recommendations Addressed in SIR and/or State Law

Policy Considerations

Central Staff has identified the following potential policy considerations and options.

1. Annual equity assessment metrics.

SPD has not yet finalized metrics to be used in evaluating use of Remotely Operated Vehicles 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.

Options:

- A. Request a report on the proposed metrics by a date certain.
- B. Take no action.
- 2. Mitigation of Civil Liberties Impacts.

The SIR provides only a boilerplate reference to SPD's general anti-bias policing policies as providing mitigation against the risk of disproportionate surveillance and/or civil liberties impacts. In the absence of data tabulating the frequency of use of the Remotely Operated Vehicles and the corresponding incident types, it is not possible to evaluate whether the technology is being used inequitably.

Options:

- A. Request that SPD report on the deployment of Remotely Operated Vehicles by incident type and location for the past three years and identify any disproportionate impacts.
- B. Take no action.

Attachment:

- 1. Surveillance Working Group Working Group Recommendations: SIR Citations, Current Law, and CTO and SPD Responses
- cc: Esther Handy, Director Aly Pennucci, Deputy Director Brian Goodnight, Supervising Analyst



Attachment 1. Surveillance Working Group Working Group Recommendations: SIR Citations, Current Law, and CTO and SPD Responses

Working Group Recommendation		Whether/How Addressed by SIR, CTO or SPD and/or Current Law
1.	Prohibit the use of Remotely Operated Vehicles to deploy weapons.	CTO Response: " any use outside of what is codified in the SIR, in this case weaponization of Remotely Operated Vehicles, would be in violation of the ordinance."
2.	Require a court-ordered warrant to use Remotely Operated Vehicles to surveil any members of the public.	 SIR §3.2 There is no legal standard or condition for the use of these cameras in non-protected public areas, such as a hotel hallway or public waterway if the use of the camera is to occur inside a protected area, such as in a person's home or property, absent exigent circumstances, or consent, a signed warrant is obtained from a judge. Appendix E: Remotely Operated Vehicles do not record without a
		warrant.
3.	Prohibit SPD from using cell phones to record the livestream on the Remotely Operated Vehicle display.	Not addressed in the SIR.
		Per SPD, recordings created by use of department-issued devices would be covered by SPD's Policy.12.040, Department-Owned Computers, Devices & Software. SPD's SPD Policy 7.090 Pol-2, Photos and Videos Created by Employees prohibits employees from creating or storing photo or video evidence on personal devices.
4.	Clearly define the incident types for which Remotely Operated Vehicles may be used, how they may be used and usage limits.	SIR §1, 2, 3 and 4 provide this information
		SIR §7.4 No information, images, or audio are recorded by any of the SWAT or Arson/Bomb Remotely Operated Vehicles.
5.	Provide strong access controls for Remotely Operated Vehicles.	SIR §4.1 This equipment is securely stored and accessible only to the specified units for use in their operations.
		SIR §6.1 No person, outside of SPD, has direct access to the Remotely Operated Vehicles or the data while it resides in the device.
6.	Require immediate deletion of any data collected via Remotely Operated Vehicles not needed for an investigation.	SIR §5.1 No images or data are stored or retained by Remotely Operated Vehicles used by SWAT or Arson/Bomb units. The Harbor unit Remotely Operated Vehicles store video and sonar imagery on a hard drive, which is periodically deleted when it is nearing capacity. Information retained for investigation is saved in SPD's Evidence system.
7.	Require that data collected via Remotely Operated Vehicles never leave SPD-owned equipment/	SIR §4.2 Only images directly related to the specific search and recovery are manually exported from the Remotely Operated Vehicle's onboard hard drive if requested by SPD detectives for follow up investigation.
8.	Make publicly available the number of people who have access to Remotely Operated Vehicles and the purchase orders and contracts for each of the Remotely Operated Vehicles.	This information is not provided in the SIR.

Working Group Recommendation		Whether/How Addressed by SIR, CTO or SPD and/or Current Law
9.	Make specific information available monthly about each Remotely Operated Vehicle, its use and how and why data gathered from an Remotely Operated Vehicle has been shared.	SIR §2.3 identifies the manufacturers of the Remotely Operated Vehicles used by SPD. Monthly reports on Remotely Operated Vehicle usage are not addressed in the SIR.
10.	Provide adequate and standardized training for all personnel who use these Remotely Operated Vehicles, including a privacy component.	 SIR §3.3 Authorized users of Remotely Operated Vehicles are trained in their appropriate use and application. SIR §7.2 SWAT, Arson/Bomb, and Harbor unit personnel are trained on the proper use of the Remotely Operated Vehicles utilized by their unit.
11.	Keep an audit log of user actions for Remotely Operated Vehicles and produce a publicly available annual audit report about SPD's use of Remotely Operated Vehicles	 SIR §5.4 SPD's Intelligence and Analysis Section reviews the audit logs and ensures compliance with all regulations and requirements. CTO Response: Technology audits, including deployment of Remotely Operated Vehicles, may be conducted by the Office of the Inspector General, the federal monitor, and/or by the Audit, Policy, and Research section within SPD at each entity's discretion. The Surveillance Ordinance mandates yearly auditing of these technologies by the Office of Inspector General.