Surveillance Usage Review: Seattle Department of Transportation Closed Circuit Television (CCTV) Traffic Cameras

June 30, 2021

Megumi Sumitani

David G. Jones, City Auditor

Seattle Office of City Auditor

Surveillance Usage Review: Seattle Department of Transportation Closed Circuit Television (CCTV) Traffic Cameras

Report Highlights

Background

The Seattle Department of Transportation's (SDOT) Closed Circuit Television (CCTV) Traffic Cameras technology is used to monitor traffic conditions in Seattle. SDOT traffic engineers view the cameras to detect and respond to traffic issues, and through the public website that transmits live feed from the cameras, the public can view traffic conditions at many locations throughout the city to make travel decisions. Traffic cameras are also used to respond to emergencies and to monitor major city-wide events.

What We Found

We concluded that overall, SDOT is in general compliance with the technology's use pursuant to its Surveillance Impact Report (SIR) and Consolidated Surveillance Impact Report (CSIR). However, we identified several areas that SDOT should address, including policy inconsistencies and user training. We also concluded that the City of Seattle (City) has no control over what users may do with CCTV data because it is publicly streamed. Also, SDOT does not have written agreements with the City departments that have access to the CCTV cameras to not record what they view through the cameras.

Recommendations

We make 19 recommendations to address SDOT's use of its CCTV technology relative to compliance with the adopted SIR and CSIR. They include: addressing and resolving inconsistencies in operational policies and training documents, clarifying policy terminology, executing technology and data use agreements with non-SDOT users, and increased user training.

WHY WE DID THIS AUDIT

This audit is required by: Ordinance 125376, which requires the City Auditor to conduct an annual review of City departments' use of City Council-approved non-police surveillance technologies, and Ordinance 125936, which approved the use of SDOT's CCTV technology.

HOW WE DID THIS AUDIT

To accomplish the audit's objectives, we:

- Reviewed the 2018 Surveillance Impact Report (SIR) and 2019 Condensed Surveillance Impact Report (CSIR), attachments to Ordinance 125936
- Interviewed SDOT officials who manage and operate CCTV technology
- Analyzed data pertaining to complaints and concerns about CCTV technology and demographic information of CCTV camera locations
- Obtained cost data for the use of CCTV technology

Seattle Office of City Auditor
David G. Jones, City Auditor
www.seattle.gov/cityauditor

We also recommend that SDOT engage cybersecurity experts to conduct regular security assessments of the CCTV traffic system to identify and address data security and the risk of CCTV traffic camera data being inadvertently or improperly shared. This work could be done by the City of Seattle's Information Technology Department or by an independent cybersecurity consultant.

For a complete list of our recommendations, please see Appendix D.

Department Response

In their formal, written response to our report, SDOT stated that they concur with our 19 recommendations and will take steps to resolve each by the end of 2021. We include SDOT's response in Appendix A.

In its formal response to our report, the Executive said it will be challenging without additional funding to implement our recommendation concerning engaging cybersecurity experts to conduct regular security assessments of the CCTV traffic system (Recommendation 5). We include the Executive's response in Appendix C.

TABLE OF CONTENTS

INTRODUCTION

Section Summary

- This surveillance usage review, including what the review should cover, was required by Ordinance 125376.
- The use of Seattle Department of Transportation Closed Circuit Television traffic cameras technology was approved by the Seattle City Council via Ordinance 125936 in September 2019. The ordinance adopted the Surveillance Impact Report (SIR) and the Condensed Surveillance Impact Report (CSIR) that specify the procedures and protocols for this approved technology.[1]

Audit Overview

This audit on the Seattle Department of Transportation's (SDOT) use of closed circuit television (CCTV) traffic cameras is required by Seattle Municipal Code 14.18.060 (Ordinance 125376 "Acquisition and Use of Surveillance Technologies"), which requires the City Auditor to conduct an annual review of the surveillance technologies used by all City of Seattle (City) departments, except for those used by the Seattle Police Department. The review is to cover the extent to which departments are following the requirements of Chapter 14.18 and the terms of approved Surveillance Impact Reports (SIRs).

The ordinance states that the review should include, but not be limited to the following:

A. How surveillance technology has been used, how frequently, and whether usage patterns are changing over time;
B. How often surveillance technology or its data are being shared with other entities, including other governments in particular;
C. How well data management protocols are safeguarding individual information;
D. How deployment of surveillance technologies impacted or could impact civil liberties or have disproportionate effects on disadvantaged populations, and how those impacts are being mitigated;[2]

[1] Ordinance 125376, 14.18.020F City Council approval for acquisition of surveillance technologies: Following Council approval of the acquisition and the terms of the SIR, the department may acquire and use the approved surveillance technology only in accordance with the procedures and protocols set forth in the SIR.

[2] In its entity, Ordinance 125376, Section 14.18.060, D states: How deployment of surveillance technologies impacted or could impact civil liberties or have disproportionate effects on disadvantaged populations, and how those impacts are being mitigated, including, for SPD, an examination of whether deployments are pursuant to warrants or not and how The Seattle Police Department's (SPD) surveillance technology is used to analyze patterns to predict suspect, individual, or group-affiliation behavior. Here, we omitted the reference to SPD because this technology is not an SPD technology. The Inspector General for Public Safety is responsible for the annual surveillance usage review for SPD technologies.

E. A summary of any complaints or concerns received by or known by departments about their surveillance technology and the results of any internal audits or other assessments of code compliance; and
F. Total annual costs for use of the surveillance technology, including personnel and other ongoing costs.

In their response to our report, the Seattle Department of Transportation (SDOT) stated that they concur with our 19 recommendations and will take steps to resolve each by the end of 2021.

We thank individuals from City of Seattle departments, and other outside entities for their cooperation and assistance. They are listed in Appendix K. The audit team for this project included Melissa Alderson and Megumi Sumitani.

Legislative Background

SDOT's CCTV traffic cameras technology is a legacy technology that predates Seattle's "Surveillance Ordinance" (Ordinance 125376) that was approved by the Seattle City Council on July 2017. The Surveillance Ordinance is intended to provide greater transparency to the City Council and the public when a City department acquires or uses surveillance technology that raises concerns about privacy or other civil liberties and involves new or legacy technologies that require City Council review and approval for their use. The City Council approved the use of SDOT's CCTV traffic cameras as a surveillance technology via Ordinance 125936 in September 2019.

Audit criteria and numbering of policies in SIR

We used the operational policy statements in the CCTV Traffic Cameras Surveillance Impact Report (SIR) and CCTV Condensed Surveillance Impact Report (CSIR) as the criteria to assess the evidence we gathered (e.g., from interviews) about whether the technology is being used in accordance with legislative requirements.

The operational policies in the adopted CCTV Surveillance Impact Report (SIR) are not numbered. Please refer to Appendix E for the numbers we assigned to the operational policies in the CCTV SIR and to which we refer in this report. In Appendix E we also list the section in this report where we discuss and assess compliance for each operational policy.

A. SURVEILLANCE TECHNOLOGY USE AND TRENDS

Section Summary

To understand how the CCTV traffic camera technology is being used, how frequently, and whether usage patterns have changed over time, we interviewed knowledgeable SDOT officials who manage and operate SDOT's CCTV technology and visited SDOT's Transportation Operations Center (TOC) in the Seattle Municipal Tower. We found that:

- The CCTV system is used to monitor general traffic conditions on public rights of way, traffic conditions after an unplanned incident, and traffic conditions affected by a planned event.
- Traffic cameras are powered and providing streaming video 24 hours a day and 365 days a year unless there is a technical issue that interferes with a camera's operation.
- The primary user of this technology is SDOT's TOC whose staff respond to traffic incidents throughout Seattle. Traffic cameras are also used by other City departments to respond to emergencies and to monitor major city-wide events.
- The images seen by SDOT traffic cameras are available to the public from the website (http://web6.seattle.gov/travelers/) either as a live feed or as static images that are updated about every three to five minutes.
- As of June 2020, SDOT operated 284 CCTV cameras but this number may not be accurate as new cameras added through capital improvement projects are not consistently captured in the camera inventory.

What is CCTV traffic camera technology?

SDOT CCTV Traffic Cameras
Source: Seattle Department of Transportation Traffic Cameras Fact Sheet

A traffic camera is a dedicated video camera that observes vehicular traffic. In Seattle, these cameras are installed along most major arterials, and are typically mounted on traffic poles at signalized intersections. The CCTV system includes any dedicated video or still camera owned or operated by SDOT, mounted on a traffic pole or at an intersection, that collects data about and/or images of vehicular traffic.
Traffic cameras are part of the City of Seattle's Intelligent

Transportation System (ITS)[3] that uses electronics and communications technologies on the street, and automated traffic systems, to enhance mobility for all modes by increasing the efficiency and safety of the transportation infrastructure.

When was the CCTV technology acquired?

SDOT initially acquired and deployed the technology in 2000 through a combination of a federal grant (SR-99 ITS) and City General Fund monies.

How does the CCTV technology work?

SDOT Transportation Center
Source: https://www.seattle.gov/transportation/projects-and-programs/programs/technology-program

SDOT uses three traffic cameras models: 1) Cohu Helios 3960HD, 2) Cohu RISE 4260HD, and 3) WTI Sidewinder SW720. The software used to control the CCTV traffic cameras is FLIR Cameleon ITS V.2017.1.74.

The cameras communicate using SDOT's fiber-optic ITS network, and each camera typically receives power from the nearest traffic signal cabinet. The cameras are remotely controllable so that operators can maneuver cameras using its full pan, tilt, or zoom features to best understand traffic conditions in the area. SDOT's Transportation Operations Center (TOC) receives the live video in real time and distributes information to SDOT's Response Team (SRT) trucks and to the public on Twitter and the Traveler Information Map if there is a traffic collision or some other disruptive incident or road safety issue.

Technology data flow

Live video is transmitted from the physical CCTV cameras to an internal streaming media server, called WOWZA. WOWZA is used to replicate the video streams so they can be used with other

[3] ITS core investments and infrastructure include: traffic signal controllers, cabinets, detection and displays; the citywide ITS communications network; traffic cameras that enable staff to view operations and dynamically adjust traffic signal timing if needed; DMS that provide on-street traveler information; the traveler website (www.seattle.gov/travelers) that includes congestion information, traffic advisories and traffic camera images; the Traffic Operations Center (TOC) that includes processing, monitoring, and communications equipment allowing staff to interact with the systems; and the staff that operate and maintain these assets. Source: Strategic Plan, p. 1)

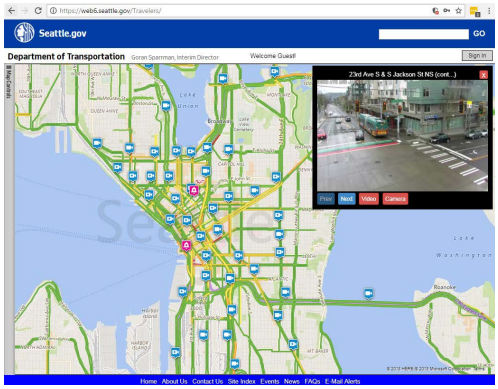
applications. The data then travels to another internal server, called the DMZ WOWZA, so that it can be prepared for live streaming. Live streaming data is transmitted from the DMZ WOWZA to the Traveler Information Map (TIM) web server, which refreshes about every three to five minutes. The Cameleon application is used by the SDOT TOC Operators and select other City department users to manage and manipulate the physical CCTV cameras, including full pan, tilt, and zoom.

Please see Appendix F for more detailed information about SDOT's CCTV traffic cameras technology.

CCTV Cameras are powered and streaming continuously

Traffic cameras are powered and providing streaming video 24 hours a day and 365 days a year unless there is a technical issue that interferes with a camera's operation.

CCTV Cameras' Data are streamed on SDOT's Traveler Information Map



Source: CCTV SIR 4.6

Data from CCTV cameras are shared with the public on SDOT's Traveler Information Map. The Traveler Information Map provides still images and streaming video from traffic cameras along with other traffic information on the website, such as congestion information, travel times, bridge opening notifications, and other alerts to help travelers to make trip decisions and to provide a full picture of traffic conditions in the city.

When connected with the website, the user has the option to select any traffic camera from the map and after a camera is selected, a still image from the camera appears; this still image is updated about every three to five minutes. When the user clicks on "video," the viewer can watch a live-stream from the selected camera that will run until the window is closed. The movement of cars, busses, bicycles, pedestrians, etc. are visible via the still images and live-stream videos. The camera resolution is purposely lowered so that still image and live-stream videos do not capture a great deal of detail, such as license plate numbers and people's faces.

CCTV system is used to monitor general traffic conditions, conditions after an unplanned incident, and traffic conditions impacted by planned events.

The CCTV system is used to monitor general traffic conditions on public rights-of-way, traffic conditions after an unplanned incident, and traffic conditions affected by planned events.

SDOT explained that "planned events" are events known in advance that will have an impact on traffic conditions because of traffic lane closures, or events that may cause congestion due to an event that brings in a lot of people and cars, e.g., large sporting events, major cultural performance events, festivals, marathons, etc.

TOC operators use CCTV traffic cameras to help manage and respond to traffic incidents and emergencies

There are seven TOC operators; each has a different shift. Operators are not assigned to specific traffic cameras; they respond to incident notifications from the Seattle Police Department's Computer Aided Dispatch (CAD) system, which is used to coordinate requests for police services.[4]

TOC operators help to manage traffic incidents with CCTV cameras. The TOC is notified of incidents from various sources, but generally, through the Seattle Police Department's (SPD) CAD dispatch system. After receiving information about a traffic incident through SPD CAD, the TOC operator verifies the incident's occurrence by going to the SDOT traffic cameras for that location to see if they can see the incident, and after assessing the incident via the traffic camera, they may decide to dispatch SDOT maintenance personnel in an SDOT Response Team (SRT) vehicle to respond to the incident. If it is a major incident that the operator was not able to verify by seeing it on a CCTV traffic camera, and SPD has already confirmed the incident, SDOT will send their SRT to the incident. Another source of information about incidents is via SPD radio dispatch by which TOC operators also get live updates from the scene.

The TOC tracks in a database, verified and non-verified incidents. Verified incidents are incidents when there was a visual confirmation of the incident by SDOT's TOC operator or the SRT; a non-verified incident is one in which there was no visual confirmation of the incident. The TOC cannot verify every incident via traffic cameras because the traffic cameras do not cover every street in Seattle. The non-verified incidents are those reported to SDOT by SPD but were not verified by SDOT.

[4] SPD's Computer-Aided Dispatch (CAD) system consists of a set of servers and software deployed on dedicated terminals in the 9-1-1 center, on SPD computers, as an application on SPD patrol vehicles' mobile data computers (MDCs), and on some SPD officers' smart phones. It assists 9-1-1 Center call takers and dispatchers to process requests for police services, collects information from 9-1-1 callers, and provides dispatchers with real-time patrol unit availability so dispatchers may dispatch appropriate patrol resources to requests for police services. Source: http://www.seattle.gov/Documents/Departments/Tech/Privacy/SPD%20Computer%20Aided%20Dispatch%20Final%20SIR.pdf, p. 3

SDOT's inventory of CCTV cameras may be incomplete

As of June 2020, SDOT reported that it operated 284 traffic cameras. However, this number may not be accurate as new cameras added through SDOT's capital improvement projects are not always activated and captured in SDOT TOC's CCTV camera inventory. SDOT told us that they are aware of this "disconnect" in their current review process with SDOT's Capital Projects Division and are taking steps to correct the process.

Finding 1

CCTV cameras installed via capital projects are not always captured in SDOT's traffic camera inventory. This results in: 1) an inaccurate inventory of CCTV cameras contributing to the City's Intelligent Transportation System (ITS), and 2) all CCTV cameras may not be connected to the Traveler Information Map website to provide traffic information to the public.

Recommendation 1

The Seattle Department of Transportation should develop and implement a process that captures all new and installed CCTV traffic cameras in the city, particularly those added via capital projects.

Compliance Summary: Surveillance Technology Use and Trends

Is SDOT in compliance with the relevant operational policies related to surveillance technology use?

The two operational policies that are relevant to the use of this technology are listed in Exhibit 1 below. Based on the preponderance of evidence we reviewed, we assessed that SDOT is in compliance with both of them.

Exhibit 1: Operational Policies Compliance Matrix, Use

Operational Policy	Is SDOT in compliance?	Recommendation(s)/ Comments
Operational Policy 1 The SDOT CCTV System will be used to monitor general traffic conditions on public rights of way, traffic conditions after an unplanned incident, and traffic conditions impacted by a planned event. **[1.0]**	**YES**	
Operational Policy 3 The CCTV System includes any dedicated video or still camera owned or operated by SDOT, mounted on a traffic pole or at an intersection, that collects data about and/or images of vehicular traffic. Cameras that detect vehicle presence and those that count and/or classify vehicles are exempted from the policies and procedures described herein. **[2.0]**	**YES**	

B. TECHNOLOGY AND DATA SHARING

Section Summary

To understand how CCTV surveillance technology and data are being shared with other entities, we interviewed SDOT Transportation Operations Center (TOC) officials who manage and operate SDOT's CCTV technology and analyzed CCTV software access records (Cameleon logs). We found that:

- CCTV technology and data are shared with the public and outside of SDOT's Transportation Operations Center, with the following SDOT functional areas and City departments: SDOT Maintenance Operations Unit Dispatch, SDOT Traffic Signal Shop, SDOT Traffic Signal Timing Engineers, Seattle Emergency Operations Center, Seattle Executive Protection Unit, Seattle Fire Alarm Center, and the Seattle Police Operations Center.
- Still images and video live-streaming from CCTV cameras are shared with the public through SDOT's Traveler Information Map.
- An operational policy in the SIR requires that the CCTV system not be used for civil or criminal enforcement purposes. SDOT reported that the system has not been used for civil or criminal enforcement purposes. However, SDOT does not have a written system/data sharing agreement with non-SDOT departments that requires them to adhere to this policy.
- We obtained and analyzed access frequency to the CCTV system by other City departments and found that from December 2019-June 2020, the Seattle Police Department accessed the system most frequently.
- We were not able to assess cybersecurity risks to the system and recommend that SDOT address them by engaging experts in the City or via consultants.

Data sharing with the public

Unless there is a technical issue that prevents a camera from operating normally, SDOT traffic cameras provide streaming video and still images to the public 24 hours a day, 365 days a year.

Frequency of data sharing with the public

SDOT tracks "device availability" by keeping data on problem cameras, i.e., cameras that are not working as intended. Over the period January 2017 – June 2020, total camera device availability averaged 90.4 percent, ranging from a low of 81 percent to a high of 96 percent.

Data use notification to public

Operational Policy 13 states: The CCTV cameras will provide a 24x7 publicly available livestream; and **Operational Policy 14** states: SDOT may disseminate live video streams over its web page, provided that users accessing the stream are notified that the system is intended to be used to monitor traffic and for no other purpose.

SDOT told us that they recognize the need to include a notification on the Traveler Information Map that the system is intended to be used to monitor traffic and for no other purpose, and that they have funding to include this notification in 2021.

Finding 2

SDOT's video streaming web page does not notify users that the system is intended to be used to monitor traffic and for no other purpose.

Recommendation 2

The Seattle Department of Transportation should prominently post a notification when the Traveler Information website is accessed that the system is intended to be used to monitor traffic and for no other purpose.

Technology and data sharing with City departments

Operational Policy 2 states: The CCTV system and data shall be used only for traffic management purposes, except for when the City's Emergency Operations Center is activated to respond to an emergency or to monitor a major city-wide event, in which case the system may be used by other City personnel (e.g. Police and Fire). The system shall not be used for civil or criminal enforcement purposes.

We met with SDOT officials to have them explain what this policy is intended to require of CCTV system users. SDOT told us that the policy's primary intent is to state that the CCTV system and data are to be used for traffic management purposes, but also that there are two instances in which CCTV system users could use the cameras for non-traffic management purposes. These two exceptions must meet either of the following two conditions: 1) emergency activation by the Emergency Operations Center (EOC), or 2) to monitor a major city-wide event. SDOT explained that non-SDOT City departments are authorized to use the CCTV system and data for any reason if it is related to traffic management or for non-traffic management purposes that meets one of the two policy exceptions.

We told SDOT that we believe that the policy does not make it clear: 1) that non-SDOT City departments are authorized to use the CCTV system and data for any reason if it is related to traffic management, 2) that there are two exceptions for using the CCTV system or data for non-traffic management purposes (i.e., 1. that the City Emergency

Operations Center is activated to respond to an emergency, or 2) to monitor a major city-wide event), and 3) what is meant by the term "to monitor a major city-wide event."

The Seattle Police Department told us that in most cases the City's EOC will not be activated during a major citywide event; instead, SPD's Seattle Police Operations Center (SPOC) will serve as a proxy for the EOC by providing hourly updates to the EOC on the event by relying, in part, on the SDOT CCTV system.

SPD stated that it would reflect actual practice for Operational Policy 2 to include in exception 1 that the SPOC, as the proxy for the City's EOC, can monitor major city-wide events as follows:

> The CCTV system and data shall be used only for traffic management purposes except for when the City's emergency Operations Center, or the Seattle Police Operations Center as its proxy is activated to respond to an emergency or to monitor a major city-wide event, in which case the system may be used by other city personnel (e.g., Police and Fire). The system shall not be used for civil or criminal enforcement purposes.

We informed SPD that adding this reference to SPD's SPOC would change a policy in the City Council approved Surveillance Impact Report, which would not be appropriate for our office to advocate for through an audit recommendation, but that should be considered by City policymakers.

See Appendix B in this report for the changes that SPD believes should be made to Operational Policy 2.

Finding 3

The wording of Operational Policy 2 does not make it clear that: 1) non-SDOT City departments can use the CCTV system and data for any reason if it is related to traffic management, 2) there are two exceptions for the use of the CCTV system for non-traffic management purposes, and 3) it is not clear what is meant by "to monitor a major city-wide event."

Recommendation 3

Operational Policy 2 should be clarified to: 1) state that non-Seattle Department of Transportation (non-SDOT) City departments are authorized to use the CCTV system and data for any reason if it is related to traffic management, 2) define the two exceptions for using the CCTV system and data for non-traffic management purposes, and 3) define what is meant by "to monitor a major city-wide event."

No system/data sharing agreement to restrict use of the CCTV system and data outside of SDOT

Operational Policy 2 also states that the CCTV system shall not be used for civil or criminal enforcement purposes.

SDOT told us they are not aware of any entity using the system for civil or criminal enforcement purposes. SPD told us that any civil or criminal enforcement would have to be initiated by officers on scene after they witnessed, in-person, a violation of law. SDOT also told us there are no written use agreements with non-SDOT departments that disallow using the CCTV system for civil or criminal enforcement purposes.

SDOT's Camera Protocol Rules of Use (see Appendix G) states that "CCTV cameras implemented by SDOT are for the purpose of traffic management, incident management and response, and public information." Although this document is provided to new non-SDOT users, it does not expressly mention that the system is not to be used for criminal or enforcement purposes, and in training new non-SDOT users, SDOT does not require new users to document their acknowledgement (e.g., by signing) of these rules.

The absence of a written agreement containing this requirement makes it more difficult for SDOT to ensure that the CCTV system or its data is not used for civil or criminal enforcement purposes by entities outside of SDOT.

Finding 4

SDOT does not obtain written assurance from non-SDOT departments that they understand and will adhere to the policy that they are not to use the CCTV system and data for civil or criminal enforcement purposes.

Recommendation 4

The Seattle Department of Transportation (SDOT) should develop and execute use agreements with non-SDOT departments that use the CCTV system and specify in the agreements that the system shall not be used for civil or criminal enforcement purposes by non-SDOT departments.

Frequency of system and data sharing with non-SDOT City departments

The SDOT TOC is the primary user of the CCTV system for the purposes of detecting and quickly responding to congestion, incidents, and other problems on City roads. As authorized by Operational Policy 4, SDOT also supports the use of the system by other SDOT units such as its Maintenance Operations Unit Dispatch and its Traffic Signal Shop, and other City entities and departments, including the Seattle Emergency Operations Center, the Seattle Police Department (SPD), and the Seattle Fire Department (SFD).

This means that individuals from non-SDOT departments, such as the EOC, SPD, and SFD, can log into the CCTV system's server (Cameleon) to view and, depending on the account's access privileges, maneuver the traffic cameras.

Our analysis of Cameleon logs provided by SDOT for the period December 2019 – June 2020 indicated that the non-SDOT department or entity that had the highest number of successful logins was SPD (142), followed by EOC (48), and SFD (37). The logs only show when Cameleon was accessed; the logs do not show which cameras were viewed or whether any cameras were moved.

Over the period December 2019 – June 2020, the month of June 2020 had the highest total number of logins (146) by these three non-SDOT departments.

Cybersecurity risks to the CCTV system

If SDOT's CCTV traffic camera system contained cybersecurity vulnerabilities, it is possible that the technology and/or data could be inadvertently or improperly shared with unauthorized parties and therefore could affect civil liberties.

We were unable to assess cybersecurity risks to the CCTV system and whether those risks are being appropriately addressed because this required technical expertise that exceeded resources that we had access to during this audit.

Answering this question is important because of risks inherent in the current data sharing structure. We determined that the City has in-house resources that could do this type of assessment, and that this expertise is provided by private contractors. The scope of such an assessment should include follow-up on the implementation progress of recommendations from the 2015 SDOT Network Security Traffic Management Risk Report. We were not able to assess the implementation status of the recommendations from the 2015 report because it also required technical expertise that exceeded resources that we had access to during this audit.[5]

The Executive, in its comments on a draft of this report, stated that although it believes that it is important to engage cybersecurity experts to conduct regular security assessments to address CCTV data security, it will be challenging to address this without additional funding allocated toward the mandate (see Appendix C.)

[5] We discuss the 2015 SDOT Network Security Service Traffic Management Risk Report in Section E: Complaints, Concerns, and Other Assessments.

Finding 5

Cybersecurity risks could result in the technology and/or data being inadvertently or improperly shared with unauthorized parties and therefore could affect civil liberties.

Recommendation 5

The Seattle Department of Transportation should engage cybersecurity experts to conduct regular security assessments of the CCTV traffic cameras system and to follow-up on the implementation progress of a 2015 network security risk report. The regular security assessments should specifically address data security and the risk of CCTV traffic cameras data being inadvertently or improperly shared. This work could be done by the City of Seattle's Information Technology Department or by an independent cybersecurity consultant.

Compliance Summary: Technology and Data Sharing

Is SDOT in compliance with the relevant operational policies related to technology and data sharing?

The four operational policies that are relevant to technology and data sharing are listed in Exhibit 2 below. Based on the preponderance of evidence we reviewed, we assessed that SDOT is in compliance with three, and is not in compliance with one.

Exhibit 2 Operational Policies Compliance Matrix, Technology and Data Sharing

Operational Policy	Is SDOT in Compliance?	Recommendation(s)/ Comments
Operational Policy 2 The CCTV system and data shall be used only for traffic management purposes, except for when the City's Emergency Operations Center is activated to respond to an emergency or to monitor a major city-wide event, in which case the system may be used by other city personnel (e.g., Police and Fire). The system shall not be used for civil or criminal enforcement purposes. **[1.0]**	**YES**	**Recommendation 3:** Operational Policy 2 should be clarified to: 1) state that non-Seattle Department of Transportation (non-SDOT) City departments are authorized to use the CCTV system and data for any reason if it is related to traffic management, 2) define the two exceptions for using the CCTV system and data for non-traffic management purposes, and 3) define what is meant by "to monitor a major city-wide event."
Operational Policy 4 SDOT only supports users of the software in the following departments or functional areas: 1. SDOT Transportation Operations Center	**YES**	

2. SDOT Maintenance Operations Unit Dispatch 3. SDOT Traffic Signal Shop 4. SDOT Traffic Signal Timing Engineers 5. Seattle Emergency Operations Center 6. Seattle Executive Protection Unit 7. Seattle Fire Alarm Center 8. Seattle Police Operations Center **[3.0]**		
Operational Policy 13 The CCTV cameras will provide a 24x7publicly available livestream. **[6.0]**	**YES**	
Operational Policy 14 SDOT may disseminate live video streams over its web page, provided that users accessing the stream are notified that the system is intended to be used to monitor traffic and for no other purpose. **[6.0]**	**NO**	**Recommendation 2:** SDOT should prominently post a notification when the Traveler Information website is accessed that the system is intended to be used to monitor traffic and for no other purpose.

C. PROTOCOLS FOR DATA MANAGEMENT

Section Summary

To understand how well data management protocols are safeguarding individual information, we interviewed SDOT Transportation Operations Center (TOC) officials who manage and operate SDOT's CCTV technology. We found that:

- SDOT's Camera Control Protocol Guidelines governs CCTV camera use and includes provisions that are intended to help ensure individual privacy protection.
- Access to the software used for the CCTV system (Cameleon) is limited to selected individuals in the SDOT TOC and City departments; when there is more than one user that needs camera control at the same time, there is a user hierarchy that applies where the higher priority user can lock out lower priority users, and use rules are set forth in SDOT Camera Control Protocol document that delineates when and in what manner cameras can be used.
- CCTV cameras are set to low resolution so that license plate numbers and faces are not clearly seen; this limits the risk of capturing Personally identifiable Information (PII).
- SDOT records videos from CCTV cameras for traffic studies and manually deletes these recordings within 10 days.
- CCTV system software (Cameleon) is not set up by SDOT to enable recording directly from it but there is nothing to prevent non-SDOT departments, or the public, from using other software to record what a CCTV camera sees.
- Once publicly streamed, there is no guarantee that data from the CCTV system will be used as intended.

Access to CCTV cameras

Access to the CCTV camera control software (Cameleon) is managed by SDOT's TOC Technical Team which grants system privileges to individual users based on their operational needs. Users' access are protected with a username and password. When the user successfully logs in to the CCTV system, a list of accessible cameras appears (all users do not have access to all cameras). The cameras accessible are user-specific. In other words, not every camera is accessible to all users; only specific cameras are accessible to each user based on the user's operational need.

There are some Cameleon user accounts that are generic; for example, in the Seattle Fire Department, where many staff may need to view the streaming from multiple CCTV cameras simultaneously.

Generic accounts are not able to move cameras; they are only able to view what the cameras are streaming.

SDOT supports Cameleon software users in the following departments or functional areas:

1. SDOT Transportation Operations Center
2. SDOT Maintenance Operations Unit Dispatch
3. SDOT Traffic Signal Shop
4. SDOT Traffic Signal Timing Engineers
5. Seattle Emergency Operations Center
6. Seattle Executive Protection Unit
7. Seattle Fire Department Alarm Center
8. Seattle Police Operations Center

CCTV camera control privileges are hierarchical

Camera control privileges are based on a user hierarchy. If two users are attempting to maneuver the same camera simultaneously, the user with the highest priority maintains control.

The SDOT TOC has the highest priority and can lock out other users from taking control of the camera. When the CCTV camera is locked by the SDOT TOC, no other user can move it. If lower level users need to use any SDOT CCTV camera, that user must contact the SDOT TOC and the CCTV camera may be released for the user to obtain camera control. This user priority hierarchy is established in SDOT's Camera Control Protocol document.

CCTV camera use rules need clarification

- SDOT's Camera Control Protocol[6] also delineates rules for using the cameras. Important use rules include:
- A statement that the "CCTV cameras and images are (to be) used in a manner consistent with the public's expectation of privacy."
- For what purpose the CCTVs shall be used: to monitor traffic conditions.
- What CCTV cameras shall be used to view: SDOT-owned roadways but not sidewalks or private property.
- Prohibited uses: operators shall not zoom in close enough to discern any information that would enable the operators to identify a member of the public, including, without limitation, license plate numbers, unless doing so is absolutely necessary to allow the operator to perform a vital component of their

[6] See Appendix G.

jobs; should it be necessary to view personally-identifiable information the operator shall terminate any dissemination of the CCTV feed to the general public before viewing such information, and shall not resume dissemination until personally-identifiable information is no longer visible; video images will not be recorded, except for compelling traffic operational needs. If they are recorded, any such recordings will be destroyed immediately after use. Recordings shall not be stored or disseminated.

We determined that two phrases in the SDOT's Camera Control Protocol are too vague to be considered firm rules. We asked SDOT's TOC Manager about these phrases and he clarified the meaning and provided several examples:

Phrase in SDOT's Camera Control Protocol	**SDOT Clarification**
"absolutely necessary"	This refers to using the camera to discern pertinent event information such as verifying a location and confirming the direction of any lanes blocked, such as zooming in to be able to read the closest street sign to verify the incident location, confirming that a traffic control plan has been set up properly, that the correct class of tow vehicle has been dispatched to the incident, and to detect oil on the roadway.
"compelling traffic operational needs"	This refers to an approved traffic study, such as for traffic safety analysis and verifying the effectiveness of operational changes (e.g., signal timing adjustments, lane marking changes).

Finding 6

It is not clear in SDOT's Camera Control Protocol the meaning of the language: 1) "absolutely necessary to allow the operator to perform a vital component of their jobs" with respect to operators zooming in closely enough to discern personally-identifiable information, and 2) "compelling traffic operational needs" with respect to the prohibition of recording video images. Without explicit guidance, TOC Operators could control cameras and record video in way that conflicts with the SIR's intent.

Recommendation 6-1

The Seattle Department of Transportation should clarify in its Camera Control Protocol what is meant by the term "absolutely necessary to allow the operator to perform a vital component of their jobs" with respect to operators zooming in close enough to discern personally identifiable information. Providing examples of what are included and excluded could help to clarify the meaning of this term.

Recommendation 6-2

The Seattle Department of Transportation should clarify in its Camera Control Protocol what is meant by the phrase "compelling traffic operational needs" with respect to the prohibition of recording video images. Providing examples of what are included and excluded could help to clarify the meaning of this phrase.

Inconsistency between SDOT Camera Control Protocol and Operational Policies 1 and 5

Operational Policy 5 states: CCTV operators must make reasonable efforts to limit data capturing to video or still images of traffic conditions within a **public right of way** or other publicly owned property. This is consistent with **Operational Policy 1,** which also states that the system will be used on **public rights of way**.

However, the SDOT Camera Control Protocol states "CCTVs shall be used to monitor conditions on **SDOT-owned roadways** and shall not be used to monitor conditions on the **sidewalk** or on private property." According to the Seattle Right-of-Way Improvements Manual, sidewalks are part of the street right-of-way. But the SDOT Camera Control Protocol states that the system shall not be used to monitor condition on the sidewalk, which is inconsistent with SIR Operational Policies 5 and 1.

SDOT told us that they will modify the policies and the Camera Control Protocol to be consistent with each other, including removing the statement, "and shall not be used to monitor conditions on the sidewalk" from the Camera Control Protocol to recognize the need to monitor conditions on sidewalks because traffic collisions often end up on sidewalks.

Finding 7

The SDOT Camera Control Protocol states: "CCTVs shall be used to monitor conditions on SDOT-owned roadways and shall not be used to monitor conditions on the sidewalk or on private property."

However, both Operational Policy 5 and Operational Policy 1 refer to the use of cameras within or on public rights of way. Inconsistencies in the Camera Control Protocol document and Operational Policies can result in CCTV camera users operating the cameras in different ways, some of which may conflict with the CCTV SIR.

Recommendation 7

The Seattle Department of Transportation (SDOT) should resolve the inconsistencies in operational policies in the SIR and the Camera Control Protocol regarding references to where cameras may be used to view/monitor conditions (i.e., SDOT-owned roadways, public rights-of-way, and/or sidewalks).

Omission of CSIR operational policy concerning personally identifiable information in the CCTV SIR

CSIR 3.0, #3 states: To the extent feasible, CCTV public feed must be terminated during such times as personally identifiable information is visible on the feed.

This operational policy is not mentioned in the CCTV SIR.

The SDOT TOC Operations Manual states that the TOC should minimize the need to disable live video streams and, to avoid showing a graphic incident, point the camera away from the incident or focus on the roadway closure. However, if disabling live video streams is necessary, the TOC Manager or SDOT's Executive Duty Officer (EDO) must approve the disabling of the live feed. If approved, the TOC Operator should call the TOC Tech Support on-call phone and pass on the request. When the feed no longer needs to be disabled, the TOC Operator shall call the TOC Tech Support on-call to restart the video stream."

The TOC keeps "disable logs" of occurrences when the live feed is disabled. During the period 2019 – June 2020, there were no disable requests.

Finding 8

CSIR 3.0, #3 is not in the SIR.

Recommendation 8

Operational Policy 3.0, #3 in the City Council-adopted Condensed Surveillance Impact Report (CSIR) states: To the extent feasible, CCTV public feed must be terminated during such times as personally identifiable information is visible on the feed. This operational policy is not included in the City Council-adopted Surveillance Impact Report (SIR). The Seattle Department of Transportation should update the SIR and/or CSIR to make both documents consistent.

There are limits to the type and extent of data that can be collected by CCTV cameras, but data collection is ultimately

Two operational policies in the SIR (Operational Policies 5 and 6) and a provision in the SDOT Camera Control Protocol limit the type and extent of data that can be collected by CCTV cameras, but the application of these policies is dependent on operator judgement. Key text referring to operator judgement are italicized in the referenced operational policies and Camera Control Protocol, as follows:

based on operator judgement

- **Operational Policy 5:** CCTV operators must *make reasonable efforts* to limit data capturing to video or still images of traffic conditions within public right of way or other publicly owned property. **[4.0]**
- **Operational Policy 6 (and in Camera Control Protocol):** Operators *may not intentionally* use the CCTV cameras to discern any personally identifiable information *that would enable the operators to identify* a member of the public, unless doing so is necessary to allow the operator to perform a traffic management function. For any recording that does take place, the operator will *record no more information than necessary* for the traffic management function. Operators will *make reasonable efforts* to limit CCTV video or still images of traffic conditions. **[4.0]**

License plate numbers and faces are not clearly seen on Traveler Information Map because resolution on cameras are lowered

The SDOT TOC Technical Team told us that as part of setting up new cameras for deployment, the camera resolution is purposely lowered to 480 pixels so that details such as license plate numbers and faces cannot be clearly seen by anyone using the CCTV system, including what is streamed on the Traveler Information Map. Streaming is done by the video distribution system, WOWZA, with a slight delay, called low latency streaming. The lowering of the resolution at the camera limits the capturing of details of personally identifiable information on the Traveler Information Map.

Traveler Information Map provides transparency on CCTV camera use

We asked the SDOT TOC Manager how he ensures that TOC and non-SDOT operators adhere to the Rules of Use and do not aim or maneuver the cameras inappropriately. The Manager responded that there are no procedures implemented to monitor camera use in real time; SDOT relies on their training of all operators on proper system usage according to SDOT's Camera Control Protocol Rules of Use. Furthermore, there is always transparency of camera use because whatever the cameras are viewing are also streaming to the public. This includes transparency over whether a camera has been tilted or zoomed.

Inconsistent requirements for deletion of CCTV recordings

Traffic camera video is recorded and kept by SDOT for traffic studies and must be deleted after a certain amount of time. SDOT has two Operational Policies that discuss deletion of CCTV video recordings, and we noted the following inconsistency:

Operational Policy 11 states: CCTV camera videos recorded for engineering studies will be deleted within 10 days.

However, **Operational Policy 12** states: Traffic camera video recordings used for engineering studies will be destroyed after 10 days and may be accessed only by SDOT employees.

The two operational policies are inconsistent as to when the recordings should be deleted (deleted within 10 days vs. destroyed after 10 days). This discrepancy should be resolved.

Also, although not mentioned in the CCTV operational policies, there are further inconsistent references in the SIR to of when recordings should be deleted, as follows:

- SIR 5.1 states: "…all recordings will be destroyed immediately after use."
- SIR 5.4 states: "…the TOC Technical Team is responsible for deleting any video file 10 days after the file's last "date modified" value has been reached."
- SIR 3.3 referring to the Camera Use Policy, it states: "Video images will not be recorded, except for compelling traffic operational needs. If they are recorded, any such recordings will be destroyed immediately after use. Recordings shall not be stored or disseminated."

Finding 9

There are inconsistencies in the operational policies in the SIR and other references in the SIR regarding when CCTV recordings should be deleted, i.e., Operational Policies 11 and 12, SIR sections 5.1, 5.4, and the Camera Use Policy (SIR section 3.3).

Recommendation 9

References in the Surveillance Impact Report and the Seattle Department of Transportation's (SDOT) CCTV Camera Use Policy regarding the destruction/deletion of files of recordings are inconsistent. SDOT should revise these policies to be consistent with one another and specify whether the number of days refers to working days or calendar days.

Recording CCTV streamed video

SDOT officials explained that they record CCTV traffic camera footage for traffic engineering studies such as transit channelization studies and "Block the Box" studies, via its internal server and that they keep a log of all recording requests as well as a deletion log of when the recordings were deleted. SDOT provided us their recording and deletion logs for 2019 – June 2020.

No use agreement to restrict recording of publicly streamed CCTV video

However, there is nothing to prevent non-SDOT departments or the public from recording streamed video using a third-party recording application on their computer.

Finding 10

There is nothing to prevent non-SDOT Cameleon users or the public to record what they see on the traffic cameras using a third-party recording application on their computer.

Recommendation 10-1

The Seattle Department of Transportation should include in its CCTV system data sharing/use agreements with other City departments language that they should not record what they view through the cameras.

Recommendation 10-2

The Seattle Department of Transportation should consult with the City Attorney's Office to determine whether a notification could be added to the Traveler Information website that recording from this public website should be prohibited.

No formalized training for non-SDOT Cameleon users

Operational Policies 7[7] and 10[8] require that training be completed for Cameleon users. The TOC Manager told us that new TOC employees are trained following a structured New Employee Training Program and the TOC Operations Manual serves as a training resource for new employees during the on-boarding process. The TOC Manager told us that SDOT does not document when this training was completed.

However, SDOT does not provide the same formal, structured training to non-SDOT Cameleon users, but instead provides it on an as-needed basis. Not all aspects of the TOC's full training may be necessary for non-SDOT users; however, appropriate training for non-SDOT users should be developed, formalized, and documented as to when the training was completed.

Finding 11

No structured training program for non-SDOT Cameleon users.

Recommendation 11

The Seattle Department of Transportation (SDOT) should develop a structured training program, including a schedule for periodic re-training, for non-SDOT users of Cameleon that is appropriate to their use of the system.

[7] **Operational Policy 7** states: SDOT shall develop standard training for operation of the SDOT CCTV camera system and handling and deletion of data collected by it in accordance with this Section and with any additional applicable SDOT policies, and only employees who have undergone such training may access or use the SDOT CCTV traffic camera system.

[8] **Operational Policy 10** states: Any City employee, whether an internal SDOT employee or other departmental user of the System, and those accessing data collected by the System, must complete training prior to using the system or accessing data collected by it.

Finding 12

The TOC does not document when training has been completed for Cameleon users.

Recommendation 12

The Seattle Department of Transportation's (SDOT) Transportation Operations Center should maintain documentation of when training was completed for all Cameleon users (within and outside of SDOT).

Cameleon logs

Cameleon (v,2017.1.74) is the software application used for CCTV camera access and camera control. The SDOT TOC Technical team provided us logs that we were able to review for the period December 2019 – June 2020.

Operational Policy 9 states: SDOT must keep a log of all access to and operations of the CCTV, including streaming stop/start, recording dates and topics. If new equipment provides capability to log camera adjustments, SDOT will revise its procedure accordingly. **[4.0]**

We asked SDOT about the individual components of this operational policy. We were informed that:

- "a log of all access to…the CCTV" refers to the recording of when and who (users) accessed (logged-into) Cameleon.
- We examined Cameleon logs from December 2019-June 2020. These logs recorded the usernames and each instance Cameleon was accessed.
- "a log of all operations of the CCTV" refers to the recording of the maneuvering of cameras while logged-in.
- The current Cameleon software (v.2017.1.74) does not log the maneuvering of cameras. SDOT informed us that the next Cameleon version that will be deployed will log maneuvering of cameras by users.
- Regarding "streaming start/stop," one SDOT staff told us she believes that streaming start is referring to when new cameras are deployed, and that streaming stop refers to when the cameras are decommissioned. The TOC Manager however, believes that it is referring to "SDOT's Disable Live CCTV Feed Policy" when the TOC disables all or specific live CCTV feeds from the Traveler Information Map website. This action must be approved by the TOC Manager or SDOT's Executive Duty Officer.
- SDOT provided us their "Disable Logs" for 2019 – June 2020. There were no instances over that period when the public feeds were disabled. The TOC Manager told us that he believes the only time the public feed was disabled was when President

Obama was in the Seattle area and the Secret Service asked the TOC not to publicly stream his travel route.

- "Recording dates and topics" refers to the CCTV Recording Request Logs documenting recording requests and the reasons they were requested, e.g., for a traffic study.

Cameleon logs are subject to the City's General Retention Schedule

SDOT provided us Cameleon logs starting from December 2019. They were not able to provide them before December 2019, because the logs were not stored in a server. These logs are important because they provide an audit trail of who accessed the CCTV cameras and when and is a requirement in the operational policy.

Cameleon logs are also subject to the City's General Records Retention Schedule. We met with the City's Records Manager who informed us that system activity/usage/access logs are considered "System Usage – Monitoring" records and are subject to a retention schedule of 1 year after activity. And because Cameleon logs are referenced in the City Council-adopted CCTV Surveillance Impact Report attached in the ordinance that authorized the approval and uses of the CCTV technology, the City Records Manager stated that the City would want to ensure that the logs are kept in accordance with their retention requirement.

Furthermore, the City's General Records Retention Schedule also states that "records involved in investigations, audits, litigation or public disclosure requests must be maintained until all related actions are complete." The City Auditor's Office is required to submit an annual usage review of this technology each September covering the data and activities of the previous year. Our office will need to review Cameleon logs to complete the usage reviews, which may mean that the retention requirement should extend to at least two years.[9]

SDOT should work with the City Records Manager and the City Auditor to set a retention period for retaining Cameleon logs to meet both the City's Records Retention Schedule and maintain availability of the logs for the City Auditor's Office to complete annual surveillance usage reviews of the CCTV technology as required by Ordinances 125376, 125679, and 125936.

Finding 13

As required by Operational Policy 9, and the City's General Records Retention Schedule, SDOT did not keep Cameleon logs before November 2019.

[9] Ordinance 125679. Section 5 excerpt: Surveillance usage reviews in subsequent years shall be filed in September and cover the data and activities of the previous year.

Recommendation 13

The Seattle Department of Transportation should work with the City Records Manager and the City Auditor to identify the appropriate retention and ensure it is listed correctly on the SDOT retention schedule so that Cameleon logs meet both the City's recordkeeping requirements and maintain availability of the logs for the City Auditor's Office to complete annual surveillance usage reviews of the CCTV technology.

Finding 14

Operational policy 9 is unclear when it refers to multiple logging requirements without specifying what requirements need to be documented in which logs (e.g., Cameleon logs, Disable Live CCTV Feed logs, and Recording Request logs).

Recommendation 14

The Seattle Department of Transportation should rewrite Surveillance Impact Report Operational Policy 9 to clarify which logs the requirements are referring to.

CCTV cameras are checked once daily to ensure that they are positioned at home preset

Section 8.2.1 of the Surveillance Impact Report states:
"Cameras are set to typically point in a particular direction (called home preset) that would best aid commuters who might access the video from the internet to make trip planning decisions. Twice a day, TOC Operators review each camera to confirm that none have drifted from that position due to wind or vibration. If that has occurred, the TOC Operator will reposition the camera and again save the home preset."

We met with SDOT TOC officials to confirm whether each CCTV camera is checked twice daily to ensure that each is set at their home preset position. TOC officials told us that the cameras are not checked twice daily, but that they are checked once per day. The TOC performs a daily formal system check of each CCTV camera each evening and reports on camera issues that need to be followed up by its Technical Team. As part of this daily check, each camera is checked to ensure that it is in its home preset position and repositioned to its home preset if necessary. This check of the cameras' preset position, however, is not documented in the daily system check report, as only issues that require follow-up are reported in it. Also, in the course of their normal work, if TOC Operators notice that any camera is not positioned at its home preset, the operator will position the camera to its home preset. TOC officials told us that an added control is that the cameras automatically return to their home preset position after 5 minutes of inactivity.

Finding 15

Instead of twice daily, CCTV cameras are checked once per day, which is contrary to what is stated in Section 8.2.1 of the CCTV Surveillance Impact Report.

Recommendation 15

Section 8.2.1 in the Closed-Circuit Television Camera (CCTV) Surveillance Impact Report should be revised to accurately reflect the current practice of each camera being checked once daily by Seattle Department of Transportation CCTV camera operators to ensure that it is in its home preset position.

Compliance Summary: Protocols for Data Management

Is SDOT in compliance with the relevant operational policies related to data management protocols?

The eight operational policies that are relevant to protocols for data management are listed in Exhibit 3 below. Based on the evidence we reviewed, we determined that SDOT was in compliance with three operational policies, was not in compliance with three, and for two, we were unable to determine SDOT's compliance due to the lack of SDOT criteria for making such an assessment.

Exhibit 3: Operational Policies Compliance Matrix, Protocols for Data Management

Operational Policy	Is SDOT in compliance?	Recommendation(s)/ Comments
Operational Policy 5 CCTV operators must make reasonable efforts to limit data capturing to video or still images of traffic conditions within a public right of way or other publicly owned property. **[4.0]**	**NOT ASSESSED**	• We did not assess whether operators make reasonable efforts to appropriately limit camera use because there are no procedures in place to monitor camera use in real-time; reliance is on the training of operators. • This operational policy refers to "public right of way" and "other publicly owned property", that are not consistent with other operational policies and the Camera Control Protocol in referencing where cameras may be used to view/monitor. This inconsistency should be resolved; see **Recommendation 7** as follows: • **Recommendation 7:** The Seattle Department of Transportation should

		resolve the inconsistencies in operational policies in the SIR and the Camera Control Protocol regarding references to where (i.e., SDOT-owned roadways, public rights-of-way, and sidewalk) cameras may be used to view/monitor conditions.
Operational Policy 6 Operators may not intentionally use the CCTV cameras to discern any personally identifiable information that would enable the operators to identify a member of the public, unless doing so is necessary to allow the operator to perform a traffic management function. For any recording that does take place, the operator will record no more information than necessary for the traffic management function. Operators will make reasonable efforts to limit CCTV video or still images of traffic conditions. **[4.0]**	**NOT ASSESSED**	We did not assess whether operators make reasonable efforts to appropriately limit camera use because there are no procedures in place to monitor camera use in real-time; reliance is on the training of operators.
Operational Policy 7 SDOT shall develop standard training for operation of the SDOT CCTV Traffic Camera System and handling and deletion of data collected by it in accordance with this Section and with any additional applicable SDOT policies, and only employees who have undergone such training may access or use the SDOT CCTV Traffic Camera System. **[4.0]**	**YES**	Training is provided, but we made the following recommendations to strengthen the current training program: • **Recommendation 11:** SDOT should develop a structured training program, including a schedule for periodic re-training, for non-SDOT users of Cameleon that is appropriate to their use of the system. • **Recommendation 12:** The Seattle Department of Transportation should maintain documentation of when training was completed for all Cameleon users (within and outside of SDOT).
Operational Policy 8 The SDOT CCTV System will not be used to collect any data other than the following: • Live-streamed feed of current traffic conditions • Recorded video of traffic for engineering studies	**YES**	SDOT informed us that they use the system for the collecting data as listed in the three bullets, but because the newest CCTV cameras have expanded data collection capabilities, SDOT will seek to update this operational policy to reflect the more sophisticated, complex types of data the cameras can collect and report on. These

• Still images of traffic conditions used in training materials or included in social media **[4.0]**		types of data include traffic volumes, directional flow, vehicle classification, traffic speed, etc., which are very useful for internal traffic engineering and planning studies, particularly with respect to the City's Vision Zero program (achieving zero traffic fatalities and severe injuries on city streets by 2030).
Operational Policy 9 SDOT must keep a log of all access to and operations of the CCTV, including streaming stop/start, recording dates and topics. If new equipment provides capability to log camera adjustments, SDOT will revise its procedure accordingly. **[4.0]**	**NO**	Although SDOT complies with two out of three of the items discussed in this operational policy, we assessed this operational policy as "not in compliance" because it is unclear and should be re-written. **Recommendation 13:** The Seattle Department of Transportation should work with the City Records Manager and the City Auditor to identify the appropriate retention and ensure it is listed correctly on the SDOT retention schedule so that Cameleon logs meet both the City's recordkeeping requirements and maintain availability of the logs for the City Auditor's Office to complete annual surveillance usage reviews of the CCTV technology. **Recommendation 14:** The Seattle Department of Transportation should rewrite SIR Operational Policy 9 to clarify which logs the requirements are referring to.
Operational Policy 10 Any City employee, whether an internal SDOT employee or other departmental user of the System, and those accessing data collected by the System, must complete training prior to using the system or accessing data collected by it. **[4.0]**	**YES**	Training is provided by SDOT, but we made the following recommendations to strengthen the current training program: • **Recommendation 11:** SDOT should develop a structured training program, including a schedule for periodic re-training, for non-SDOT users of Cameleon that is appropriate to their use of the system. • **Recommendation 12:** The Seattle Department of Transportation's (SDOT) Transportation Operations Center should maintain documentation of when training was completed for all

		Cameleon users (within and outside of SDOT).
Operational Policy 11 CCTV camera videos recorded for engineering studies will be deleted within 10 days. **[5.0]** **(INCONSISTENCY: WITHIN 10 DAYS VS AFTER 10 DAYS IN NEXT OP)**	**NO**	We assessed this operational policy as "out of compliance: because this policy is inconsistent with Operational Policy 12. **Recommendation 9:** References in the SIR and SDOT's CCTV Camera Use Policy regarding the destruction/deletion of files of recordings are inconsistent. SDOT should revise these policies to be consistent with one another and specify whether the number of days refers to working days or calendar days.
Operational Policy 12 Traffic Camera video recordings used for engineering studies will be destroyed after 10 days and may be accessed only by SDOT employees. **[5.0]**	**NO**	We assessed this operational policy as "out of compliance" because this policy is inconsistent with Operational Policy 11, **Recommendation 9:** References in the SIR and SDOT's CCTV Camera Use Policy regarding the destruction/deletion of files of recordings are inconsistent. SDOT should revise these policies to be consistent with one another and specify whether the number of days refers to working days or calendar days.

D. CIVIL LIBERTIES IMPACT

Section Summary

- In terms of civil liberties impacts caused by the CCTV system cybersecurity vulnerabilities, we could not conclude whether CCTV technology had a negative effect on civil liberties or had disproportionate effects on disadvantaged populations because this required information technology security expertise that we did not have access to during this audit.
- In terms of where CCTV traffic cameras are located in Seattle, we also could not conclude whether CCTV technology had a negative effect on civil liberties or disproportionate effects on disadvantaged populations because although SDOT has a process to determine where to deploy new CCTV cameras, it does not have a process to document the rationale for the decisions about where to locate the cameras. However, we mapped the locations of SDOT's CCTV cameras in Seattle, which indicated that SDOT placed CCTV cameras in areas based on traffic volume, and they are concentrated along major arterials in the city. The top four census tracts that contain the most CCTV cameras are in the broader Downtown area, and SDOT told us this is because of the high traffic volume and topography of those neighborhoods.
- In terms of use of the CCTV technology, an ACLU-Washington representative told us that there was one instance during which CCTV traffic cameras were used to zoom in on the faces of protesters over the summer of 2020 and that this deters people from exercising their constitutionally protected right to protest. We discuss this alleged misuse of the CCTV traffic cameras as a complaint in Section E of this report.

What are civil liberties concerns about SDOT CCTV traffic cameras?

We asked ACLU-Washington representatives about whether they had concerns about the City's use of CCTV technology. They mentioned two concerns: 1) the technology's ability to remotely zoom in on the faces of individuals, and 2) the use of facial recognition technology to identify individuals on camera and for building a database of these individuals.

In October 2020, a representative of ACLU-Washington told us that they had received information about CCTV cameras being used during summer 2020 protests. The ACLU-Washington representative told us that they believe that photographs or footage of people were taken from SDOT CCTV cameras that were live-streamed on SDOT's Traveler Information webpage. We included a report of this concern

in our response to Question E: Complaints, concerns, and other assessments.

Has the deployment of CCTV traffic cameras technology affected civil liberties?

Not known. Although we did not find any evidence that this had occurred, it is possible that any cybersecurity vulnerabilities in the CCTV system could result in data being inadvertently or improperly shared with unauthorized parties and therefore impacting civil liberties.

As discussed in Section B, Data Sharing, we were unable to determine whether or not SDOT is limiting access, storing, sharing, or using CCTV data securely because this would require technical expertise that was beyond the resources we had access to during this audit. When **Recommendation 5** is implemented, the cybersecurity experts that are engaged should identify and test for potential vulnerabilities that could compromise CCTV data security and result in it being inadvertently and/or improperly shared.

As also discussed in Section B, Data Sharing, once publicly streamed, there is no guarantee that data from the system will only be used for traffic monitoring purposes by anyone, including non-SDOT departments for civil or criminal enforcement purposes.

To address non-SDOT departments' use of the CCTV system, we recommend (**Recommendation 5**) that SDOT develop and execute use agreements with non-SDOT departments who use the CCTV system requiring them not to use the system or civil or criminal enforcement purposes.

SDOT incident data categorizes free speech events as special event incidents

As discussed in Section A, Technology Use and Trends, SDOT TOC operators use CCTV cameras to help to manage traffic incidents and record incident data.

Protests and marches that block traffic are categorized as "special event incidents" by the TOC in its tracking of incident data. SDOT's TOC incident data from January 2017 – December 2019 fluctuated from year to year with most events occurring during the months of May and June. For the first six months of 2020, the highest number of special event incidents occurred in June.

Has SDOT installed CCTV traffic cameras according to policy?

Not Known. Operational Policy 15 states: SDOT will install CCTV cameras based on street transportation volumes and locations based on gaps in travel time coverage along corridors identified in SDOT's Intelligent Transportation Strategic Plan.

Between 2019-June 2020, which was the scope of this review, CCTV cameras were installed in 19 new locations. We met with SDOT

officials who told us that although they have a process for determining where to locate new CCTV cameras, it is not formally documented. See "Observations from Mapping" section for more information.

Finding 16

SDOT does not document the process and its decisions for locating new CCTV cameras.

Recommendation 16

The Seattle Department of Transportation should begin consistently documenting the rationale for its decisions about where to locate new CCTV cameras.

Observations from mapping

To analyze the geographic locations of CCTV cameras, we mapped CCTV locations pertaining to the neighborhood residential populations on two census tract layers: 1) Population Density[10] and 2) Race and Social Equity Composite Index[11] (see Appendices I and J). We also include a Traffic Flow Map from 2019 (see Appendix H).

We found that a little over half of census tracts in Seattle contain CCTV cameras. The top four census tracts that contain the most CCTV cameras are in the broader Downtown area, including the Downtown Commercial Core, Duwamish, SODO, Cascade, and

[10] Population density was calculated at the census tract-level by the Seattle Office of Planning and Community Development using population estimates from the American Community Survey 2013-2017 divided by gross land area.

[11] The Racial and Social Equity Index is a census-tract based tool to assist with implementing the City's Race and Social Justice Initiative (RSJI) and to aid in the identification of neighborhoods for City planning, program and investment priorities. The index was compiled in 2018 by the City of Seattle Demographer in the Office of Planning and Community Development. The index combines the three equally weighted sub-indices described below, with census tracts categorized by five levels (quintiles) of priority/disadvantage.

- Race, English Language Learners, and Origins sub-index: ranks census tracts by an index of three measures weighted as follows: (shares of population who are)
  - Persons of color (weight: 1.0)
  - English language learners (weight: 0.5)
  - Foreign born (weight: 0.5)
- Socioeconomic Disadvantage sub-index: ranks census tracts by an index of two equally weighted measures: (shares of population with)
  - Income below 200 percent of poverty level
  - Educational attainment less than a bachelor's degree
- Health Disadvantage sub-index ranks census tracts by an index of seven equally weighted measures:
  - No leisure-time physical activity
  - Diagnosed diabetes
  - Obesity
  - Mental health not good
  - Asthma
  - Low life expectancy at birth
  - Disability

Eastlake neighborhoods; this represents about a third of all CCTV cameras in the city.

SDOT told us that they install CCTVs according to the guidance in their Intelligent Transportation (ITS)[12] strategy. This includes placing cameras along major arterials where they would contribute the most to traffic observations, and to observe the highest volume of traffic corridors in and out of the city. SDOT will use traffic volume and traffic incident data to inform them on where more cameras might be needed. For example, SDOT told us that they installed cameras along Martin Luther King Jr Way and Rainier Ave S because of high traffic flow and an increase of traffic incidents.

Also, SDOT told us they put cameras along routes that do not have suitable alternate routes for traveling in and out of Downtown. SDOT also told us that in some parts of the city, more cameras are necessary to provide full visibility because of the physical geography and grading of the land. For example, SDOT told us they placed more cameras in Downtown Seattle because the presence of hills impedes camera visibility thus requiring more cameras to provide sufficient visibility coverage in this area of the city.

Compliance Summary: Civil Liberties Impact

Is SDOT in compliance with the relevant operational policy related to installation of CCTV traffic cameras technology?

We were not able to determine compliance with the one operational policy concerning the technology's civil liberties impact because although SDOT has a process to select locations for new CCTV cameras based on street transportation volumes and travel time gaps, the rationale for SDOT's CCTV location decisions is not documented. We recommend that SDOT develop and implement a process that documents the rational for where it installs CCTV cameras.

Exhibit 4: Operational Policies Compliance Matrix, Civil Liberties Impact

Operational Policy	Is SDOT in Compliance?	Recommendation(s)/ Comments
Operational Policy 15 SDOT will install CCTV cameras based on street transportation volumes and locations based on gaps in travel time coverage along	**NOT DETERMINED DUE TO LACK OF SDOT RECORDS**	**Recommendation 16:** The Seattle Department of Transportation should begin consistently documenting the rationale for its decisions about where to locate new CCTV cameras.

[12] SDOT's Intelligent Transportation System (ITS) is based on the ITS Strategic Plan 2010-2020. ITS uses a variety of technologies, including traffic cameras, to improve multi-modal travel across the city. (Source: https://www.seattle.gov/transportation/projects-and-programs/programs/technology-program)

corridors identified in the SDOT ITS Strategic Plan. **[RACIAL EQUITY TOOLKIT 2.0]**		

E. COMPLAINTS, CONCERNS, AND OTHER ASSESSMENTS

Section Summary

- Between 2017-June 2020, we identified one privacy or civil liberties related complaint/concern about the use of CCTV technology received by the Seattle Department of Transportation (SDOT), and none through the City of Seattle's Customer Service Bureau (CSB).
- In October 2020, we learned that the ACLU-Washington was contacted about concerns about the use of CCTV cameras during protests in the summer of 2020 when a complaint was made to SDOT's Twitter account about cameras zoomed in on a group of people.
- We found that one in-scope security assessment of SDOT's Transportation Operations Center (TOC) system was conducted over the past five years. We were not able to assess the implementation status of the recommendations from this security assessment because it would require technical expertise that was beyond the resources that we had access to during this audit.

Did SDOT receive complaints from the public about CCTV traffic cameras technology privacy concerns?

Yes. From January 2017-June 2020, SDOT directly received one complaint from the public about a CCTV traffic camera that was pointing into the windows of a building, which created a privacy concern. SDOT responded that the CCTV camera was used to "visually verify" the Battery Street Tunnel closure sign and had drifted away from its directed position. SDOT responded that they returned the camera to its regular position (this camera has since been removed with the closure of the Viaduct). SDOT told us that now all CCTV cameras are programmed to automatically return to their home positions after five minutes of inactivity.

Did the City's Customer Service Bureau receive complaints from the public about SDOT CCTV traffic cameras technology privacy concerns?

No. We did not find any complaints or concerns related to privacy or civil liberties related to CCTV cameras in the data provided by the City of Seattle's Customer Service Bureau (CSB), which is part of the Department of Finance and Administrative Services. We obtained copies of the CSB's General Inquiry Service Request data for January 2017 – June 2020.

CSB uses a cloud-based hosted application to manage and track constituents' service requests, suggestions, complaints and correspondence that are received in multiple ways, i.e., online, mobile app ("Find it, Fix It"), in person, phone, email, etc. Total CSB

service requests for 2017 were 17,267; 27,239 for 2018; 31,179 in 2019; and for January-June 2020, there were 11,234.

ACLU concerns on CCTV cameras

In October 2020, a representative of ACLU-Washington told us about a concern they had received about the use of CCTV cameras during protests in the summer of 2020. The complaint was made through a Twitter post and included a still photo of what appears to be a CCTV camera zoomed in on a group of people at a South Lake Union intersection. According to SDOT TOC officials and an ACLU-Washington official, they presumed this photo was from SDOT's Traveler Information webpage. The Twitter user making this complaint tagged the @SDOTtraffic Twitter account. We discussed this complaint with SDOT, and they told us that the TOC monitors the @SDOTtraffic account directly, and their practice is to respond to traffic related questions only. SDOT had no record of investigating or responding to this complaint.

Finding 17

SDOT had no record of investigating or responding to the above complaint received via social media. The surveillance ordinance requires the reporting of complaints or concerns about the use of the surveillance technology received or known by City departments.

SDOT does not have a process to ensure that all complaints about surveillance technologies are captured and documented in one place, regardless of how SDOT received the complaint. If SDOT does not have such a process, SDOT: 1) may not be able to investigate and respond appropriately to alleged misuse of the technology, and 2) may not be able to report all complaints and concerns received to be reported to the City Council as required by the surveillance ordinance.

Recommendation 17

To ensure that the Seattle Department of Transportation can appropriately respond to and report on complaints about misuse of surveillance technologies, it should document all complaints and concerns from all sources, including from social media.

Were there any internal audits or other assessments of code compliance concerning SDOT CCTV traffic cameras technology?

Over the past five years there have been two security assessments of SDOT TOC systems.

1. The more recent assessment examined major TOC systems and platforms, but not specific technologies used at the TOC, such as CCTV cameras, and therefore was not in our scope.

2. The other assessment was a security assessment of SDOT's traffic management network comprised of the TOC and field networks of which the CCTV system is a component. We were not

able to assess the implementation status of the recommendations from this assessment because it would require information technology and cybersecurity technical expertise that was beyond the resources that we had access to during this audit.

This follow-up work should be included as a part of **Recommendation 5** when cybersecurity experts are engaged to identify and test for potential system vulnerabilities.

F. COSTS

Section Summary

SDOT's CCTV technology costs for 2019 were about $1,078,982. This includes fully loaded personnel and ongoing maintenance costs.

What are the costs for CCTV technology?

SDOT estimated that the costs for the use of CCTV technology in 2019 was $1,078,982 and that for January 2020 through June 2020 the total estimated cost was $826,553.

	2019	January - June 2020
CCTV Personnel Costs*	$836,714	$598,754
Maintenance & Replacement Costs	$242,268	$227,799
Total Costs	**$1,078,982**	**$826,553**

Source: Seattle Department of Transportation

*fully loaded labor costs

The SDOT TOC Manager told us that SDOT replaced all the cameras that needed to be replaced for 2020 in the first half of the year, so no further maintenance and replacement costs would be incurred in 2020.

Personnel Costs

The SDOT TOC Manager explained to us that TOC staff do not track personnel hours spent working with the CCTV system. To estimate personnel costs associated with the CCTV system, the SDOT TOC Manager surveyed each TOC staff member to estimate the percentage of time spent working directly with the CCTV system in 2019 through Q2 2020 and used the loaded labor costs for each position provided by SDOT Finance to calculate estimated personnel costs attributable to CCTV technology.

Other Costs

Outside of the TOC personnel costs discussed above, costs for specific items, repair, and maintenance associated with the CCTV system are tracked. For 2019, the cost for camera maintenance by the SDOT Traffic Signal Shop was $242,268. In Q1 and Q2 of 2020, the costs were $227,799. Per the SDOT TOC Manager, the estimated installation and replacement cost is $20,000 per camera.

OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

Ordinance 125376 (the "Surveillance Ordinance"), requires the City Auditor to conduct an annual review of the City's use of surveillance technologies by all city departments except the Seattle Police Department, and Ordinance 125936, provided the City Council's approval of the use of SDOT's CCTV technology.

Ordinance 125376 states that the review for non-Police surveillance technologies should include, but not be limited to the following:

A. How surveillance technology has been used, how frequently, and whether usage patterns are changing over time;
B. How often surveillance technology or its data are being shared with other entities, including other governments in particular;
C. How well data management protocols are safeguarding individual information;
D. How deployment of surveillance technologies impacted or could impact civil liberties or have disproportionate effects on disadvantaged populations, and how those impacts are being mitigated;
E. A summary of any complaints or concerns received by or known by departments about their surveillance technology and results of any internal audits or other assessments of code compliance; and
F. Total annual costs for use of surveillance technology, including personnel and other ongoing costs.

Scope

By ordinance,[13] the scope of the usage review is to cover the data and activities of the previous year. Ordinance 125936 was signed by City Council in September 2019.

The scope of our audit was 2019 through June 2020. However, for Council question F, regarding complaints and concerns received by the department and others about CCTV technology, we examined data over the period of 2017 through June 2020.

[13] Section 6 of Ordinance 125679 amended Section 5 of Ordinance 125376 (the Surveillance Ordinance) that requires that "surveillance usage reviews (in years subsequent to 2018) shall be filed in September (of the following year) and cover the data and activities of the previous year". [Note: parens text added by auditor.]

Methodology

To accomplish the audit's objectives, we:

- Reviewed the 2018 CCTV Surveillance Impact Report (SIR) and 2019 CCVTV Condensed Surveillance Impact Report (CSIR), amendments to Ordinance 125936;
- Attended two Surveillance Technology Public Comment meetings (October 25, 2018 and November 5, 2018) during which SDOT CCTV technology was discussed so that the public could learn about the technology and to provide comments;
- Interviewed SDOT officials who manage and operate CCTV technology;
- Interviewed ACLU-Washington representatives about civil liberties concerns about CCTV technology;
- Interviewed Seattle Information Technology Department Cybersecurity/Risk Management officials about the work they have done or are doing to assess CCTV technology security risks;
- Obtained data from the Department of Finance and Administrative Services Customer Service Division on constituent service requests, suggestions, complaints and correspondence received by the City of Seattle and reviewed the data for complaints and concerns specific to CCTV technology;
- Obtained location data for CCTV cameras from the SDOT TOC and requested mapping and analysis of demographic information from Seattle Information Technology, GIS Products and Services;
- Obtained cost data for the use of CCTV technology.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable bass for our finding and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our audit objectives.

APPENDIX A

Response from the Seattle Department of Transportation

Seattle Department of Transportation

June 7, 2021

David G. Jones, City Auditor
Seattle Office of City Auditor
700 5th Avenue, Suite 2410
Seattle, WA 98104

Re: Traffic Camera Surveillance Usage Review Departmental Response

Dear David,

Thank you for working collaboratively with the Seattle Department of Transportation (SDOT) to audit our use of closed-circuit television (CCTV) traffic cameras. Audits are one way of ensuring that government is accountable to the people and neutral expert opinions are brought to bear on existing practices as a means of improving existing processes. We appreciate this thorough review of our program and agree with all of the audit's recommendations and findings, many of which validate our own program evaluations and planned improvements. We have already begun taking actions to address many of the recommendations and have plans to address all other recommendations by the end of 2021.

The audit does not identify any privacy concerns and this technology does not collect or store any personal data. These cameras are used cooperatively with the Seattle Police Department, Seattle Fire Department, and Mayor's Executive Protection Unit to maintain public safety by monitoring traffic impacts and major events, but this system is not used for civil or criminal enforcement purposes.

CCTV cameras help residents make informed decisions about their travel plans and enable our traffic engineers to make informed real-time decisions that keep the city moving. SDOT staff in our 24x7 Transportation Operations Center use these cameras to detect and respond to traffic issues, emergencies, and major events city-wide. Using a public facing website, residents can also view live video to see traffic conditions throughout the city.

The City Auditor made nineteen recommendations to address SDOT's use of its CCTV technology relative to compliance with the adopted Surveillance Impact Report (SIR) and Condensed Surveillance Impact Report (CSIR). These include addressing and resolving inconsistencies in operational policies and training documents, clarifying policy terminology, executing technology and data use agreements with other City departments, and increased user training.

SDOT concurs with all nineteen findings and will take steps to resolve each by the end of 2021:

Resolving Inconsistencies in Operational Policy and Training Documents
Eight of the recommendations are related to addressing and resolving inconsistencies in operational policies and other documents (recommendations 3,6-1,6-2,7,8,9,14,15). In response to all eight findings, SDOT will coordinate with the appropriate parties to revise those policies and documents as recommended.

Engaging Cybersecurity Experts
Recommendation 5 states that SDOT should engage cybersecurity experts to conduct

700 Fifth Avenue, Suite 3800 | PO Box 34996 | Seattle, WA 98124-4996 | 206-684-ROAD (7623) | seattle.gov/transportation

regular security assessments that specifically address data security and the risk of CCTV data being inadvertently or improperly shared. We concur and have already begun active engagement with assigned Seattle Information Technology Department (ITD) cybersecurity experts. This includes recurring meetings to review SDOT's practices and technologies while providing guidance for improving SDOT's overall security posture.

Clarifying Policy Terminology
Three of the recommendations (1,16,17) will be resolved through the creation of new standard operating procedures that will be added to our existing repository and delivered to the appropriate staff. Recommendations 2 and 10-2 will be resolved through consultation with our City Attorney's Office and subsequently updating the language on our public facing website. Regarding recommendation 13, SDOT will work with the City Records Manager and the City Auditor to set a retention period for camera use logs as suggested.

Training
The four remaining recommendations (4,10-1,11,12) relate to the creation of a structured training program and associated user agreements. SDOT has developed this training program for both SDOT and non-SDOT staff and we will ensure every user is trained using these new materials by Q4 2021.

Sincerely,

Sam Zimbabwe (Jun 7, 2021 12:03 PDT)

Sam Zimbabwe
Director

APPENDIX B

Response from the Seattle Police Department

City of Seattle
Seattle Police Department

To: David Jones, City Auditor
Megumi Sumitani, Assistant City Auditor

From: Adrian Diaz, Chief of Police

Date: June 2, 2021

RE: SDOT CCTV Traffic Cameras Report

Dear Mr. Jones and Ms. Sumitani,

Thank you for the opportunity to review your 2021 Report of the Seattle Department of Transportation's Closed Circuit Television (CCTV) Traffic Cameras, conducted pursuant to Ordinance 125376, concerning the responsibility of the City Auditor to annually review City departments' use of Council-approved non-police surveillance technologies, and Ordinance 125936, approving the use of SDOT's CCTV technology. While this technology is owned by SDOT, there are certain uses of this technology that, as you note, allow access by other departments, including the Office of Emergency Management (OEM) and the Seattle Police Department (SPD), through the Seattle Police Operations Center (SPOC), and I appreciate the opportunity to provide feedback on this access.

My comments are specific to Recommendation 3 of your report, concerning Operational Policy 2, as stated below:

Operational Policy 2

The CCTV system and data shall be used only for traffic management purposes, except for when the City's Emergency Operations Center is activated to respond to an emergency or to monitor a major city-wide event, in which case the system may be used by other city personnel (e.g., Police and Fire). The system shall not be used for civil or criminal enforcement purposes.

Recommendation 3

Operational Policy 2 should be clarified to: 1) state that non-SDOT City departments are authorized to use the CCTV system and data for any reason if it is related to traffic management, 2) define the two exceptions for using the CCTV system and data for non-traffic management purposes, and 3) define what is meant by "to monitor a major city-wide event."

Seattle Police Department, 610 Fifth Avenue, PO Box 34986, Seattle, WA 98124-4986
An equal employment opportunity, affirmative action employer.
Accommodations for people with disabilities provided upon request. Call (206) 233-7203 at least two weeks in advance.

Understanding that the City Auditor is not in a position to advocate for changes to a policy that has been Council-approved, I write separately to note that by limiting only to EOC activations the circumstances in which CCTV may be accessed in order to monitor a city-wide event, the policy excludes a majority of events for which the EOC is not "activated," but instead monitors events virtually while calling upon SPOC for situational awareness of forecasted or active events (i.e., "monitoring").

For background and context, OEM is an independent office responsible for interdepartmental collaboration during major city-wide events. SPD participates during EOC activations to support the ESF-13 (public safety) role, typically assigned to the Assistant Chief of Professional Standards, with the Captain of the Education and Training Section as a back-up. As part of its historical collaboration and support of OEM, SPOC participates in event planning meetings when a city-wide event is forecasted. During these interdepartmental meetings, SPD is responsible for providing an overview of the event(s), how the department is planning on monitoring the event, any changes to officer deployment status, and potential impacts to community or government infrastructure. It is during such meetings that the EOC operations team, with the assistance of the other ESF function representatives (of which there are a total of 15), makes the determination as to whether the EOC will be activated (or "stood up") for the event. In most cases, the determination is that the EOC will not be activated, but instead, will provide high-level situational awareness city-wide through hourly updates.

In preparation of the hourly update, the EOC SDO (Staff Duty Officer) calls SPOC to receive an update on the event, specifically to include information relating to the size of the crowd, the demeanor of the crowd, arrests that have been made, direction of travel, and other pertinent information as requested by the EOC. In order to provide such updates, SPOC personnel rely in part on SDOT's CCTV, just as they would in the event of an EOC activation. For this reason, SPD believes that Operational Policy 2 should be amended to reflect the operational practices and expectations of SPD's role with respect to the monitoring of major city-wide events, as follows:

> The CCTV system and data shall be used only for traffic management purposes, except for when the City's Emergency Operations Center, or the Seattle Police Operations Center as its proxy, is activated to respond to an emergency or to monitor a major city-wide event, in which case the system may be used by other city personnel (e.g., Police and Fire). The system shall not be used for civil or criminal enforcement purposes.

Thank you again for the opportunity to review your report and offer this brief response.

Sincerely,

Adrian Diaz
Chief of Police

APPENDIX C

Response from the Executive

From: Noble, Ben
To: Jones, DavidG; Moseley, David
Cc: Zimbabwe, Sam; Bashir, Saad; Cambridge, Jason; Emery, Adiam; Smith, Gary; Morris, Dylan; McGrath, Max; Armbruster, Ginger; Winkler, Jennifer; Schubert-Knapp, Katherine; Canzoneri, Diana; Neafcy, Kenneth; Nelson, Laurel; Boatright, Rebecca; Nelson, Dan; Sumitani, Megumi; Alderson, Melissa; Helmbrecht, Elliot; Reddy, Saroja
Subject: RE: Final Draft Review: Surveillance Usage Review of Seattle Department of Transportation Closed
Date: Wednesday, June 16, 2021 6:38:28 AM
Attachments: image002.png
image004.png
image001.png

Dear David:

Thank you for the opportunity to review your final draft report: Surveillance Usage Review: Seattle Department of Transportation Closed Circuit Television (CCTV) Traffic Cameras. And thank you for working collaboratively with the Seattle Department of Transportation and our other City of Seattle departments that access this information. While the audit did not find any privacy concerns, we appreciate your thorough review and the audit's recommendations.

Though we concur with all 19 findings and recommendations in your extensive report, we feel that it is important to mention that Recommendation 5 concerning engagement of cyber security experts to conduct regular security assessments to address data security and the risk of CCTV being improperly shared will be challenging to address without additional funding allocated toward the mandate. Seattle Information Technology Department (ITD) does not have funding to engage in the full scope of work outlined in the Auditor's report. However, active engagement and recurring meetings to review practices and technologies are still occurring between SDOT and ITD staff to improve the City's security posture.

Thank you again for the opportunity to review your report and for your ongoing work to ensure Seattle residents and travelers have confidence in the tools we are using to actively manage and make informed decisions about our transportation network.

Thanks,
Ben.

Ben Noble
Director, City Budget Office
City of Seattle | Office of the Mayor
O: 206.684-8160 | ben.noble@seattle.gov

APPENDIX D

List of Recommendations and Department Response

Recommendation 1: The Seattle Department of Transportation should develop and implement a process that captures all new and installed CCTV traffic cameras in the city, particularly those added via capital projects.	
SDOT Concurrence: Yes	Estimated Date of Completion: Q3 2021
SDOT will develop a SOP for expeditiously adding CCTV to our asset management system and operational platforms upon the completion of every project.	
Recommendation 2: The Seattle Department of Transportation should prominently post a notification when the Traveler Information website is accessed that the system is intended to be used to monitor traffic and for no other purpose.	
SDOT Concurrence: Yes	Estimated Date of Completion: Q3 2021
SDOT worked with the privacy office to craft the notification language and these changes will be deployed to the public facing map soon.	
Recommendation 3: Operational Policy 2 should be clarified to: 1) state that non-Seattle Department of Transportation (non-SDOT) City departments are authorized to use the CCTV system and data for any reason if it is related to traffic management, 2) define the two exceptions for using the CCTV system and data for non-traffic management purposes, and 3) define what is meant by "to monitor a major city-wide event."	
SDOT Concurrence: Yes	Estimated Date of Completion: Q3 2021
SDOT will implement these recommendations and define the exceptions more specifically.	
Recommendation 4: The Seattle Department of Transportation (SDOT) should develop and execute use agreements with non-SDOT departments that use the CCTV system and specify in the agreements that the system shall not be used for civil or criminal enforcement purposes by non-SDOT departments.	
SDOT Concurrence: Yes	Estimated Date of Completion: Q4 2021
SDOT has drafted user agreements and will gather signatures at the conclusion of annual training.	
Recommendation 5: The Seattle Department of Transportation should engage cybersecurity experts to conduct regular security assessments of the CCTV traffic cameras system and to follow-up on the implementation progress of a 2015 network security risk report. The regular security assessments should specifically address data security and the risk of CCTV traffic cameras data being inadvertently or improperly shared. This work could be done by the City of Seattle's Information Technology Department or by an independent cybersecurity consultant.	
SDOT Concurrence: Yes	Estimated Date of Completion: Ongoing
SDOT already has an active engagement with assigned ITD cybersecurity experts. This includes recurring meetings to review practices and technologies while providing guidance for improving SDOT's overall security posture.	

Recommendation 6-1: The Seattle Department of Transportation should clarify in its Camera Control Protocol what is meant by the term "absolutely necessary to allow the operator to perform a vital component of their jobs" with respect to operators zooming in close enough to discern personally identifiable information. Providing examples of what are included and excluded could help to clarify the meaning of this term.	
SDOT Concurrence: Yes	Estimated Date of Completion: Q3 2021
SDOT will implement this recommendation by defining the terms more specifically and providing examples.	
Recommendation 6-2: The Seattle Department of Transportation should clarify in its Camera Control Protocol what is meant by the phrase "compelling traffic operational needs" with respect to the prohibition of recording video images. Providing examples of what are included and excluded could help to clarify the meaning of this phrase.	
SDOT Concurrence: Yes	Estimated Date of Completion: Q3 2021
SDOT will implement this recommendation by defining the terms more specifically and providing examples.	
Recommendation 7: The Seattle Department of Transportation (SDOT) should resolve the inconsistencies in operational policies in the SIR and the Camera Control Protocol regarding references to where cameras may be used to view/monitor conditions (i.e., SDOT-owned roadways, public rights-of-way, and/or sidewalks).	
SDOT Concurrence: Yes	Estimated Date of Completion: Q3 2021
SDOT will resolve the inconsistencies in the SIR operational policies and Camera Control Protocol.	
Recommendation 8: Operational Policy 3.0, #3 in the City Council-adopted Condensed Surveillance Impact Report (CSIR) states: To the extent feasible, CCTV public feed must be terminated during such times as personally identifiable information is visible on the feed. This operational policy is not included in the City Council-adopted Surveillance Impact Report (SIR). The Seattle Department of Transportation should update the SIR and/or CSIR to make both documents consistent.	
SDOT Concurrence: Yes	Estimated Date of Completion: Q3 2021
SDOT will ensure Operational Policy 3.0 is consistent in both documents.	
Recommendation 9: References in the Surveillance Impact Report and the Seattle Department of Transportation's (SDOT) CCTV Camera Use Policy regarding the destruction/deletion of files of recordings are inconsistent. SDOT should revise these policies to be consistent with one another and specify whether the number of days refers to working days or calendar days.	
SDOT Concurrence: Yes	Estimated Date of Completion: Q3 2021
SDOT will ensure references to the deletion of recordings is consistent in the relevant documents and specify that the number of days refers to working days.	
Recommendation 10-1: The Seattle Department of Transportation should include in its CCTV system data sharing/use agreements with other City departments language that they should not record what they view through the cameras.	
SDOT Concurrence: Yes	Estimated Date of Completion: Q4 2021
SDOT has drafted user agreements that include this language and will gather signatures at the conclusion of annual training.	

Recommendation 10-2: The Seattle Department of Transportation should consult with the City Attorney's Office to determine whether a notification could be added to the Traveler Information website that recording from this public website should be prohibited.	
SDOT Concurrence: Yes	Estimated Date of Completion: Q3 2021
SDOT will consult with the City Attorney's Office as requested.	
Recommendation 11: The Seattle Department of Transportation (SDOT) should develop a structured training program, including a schedule for periodic re-training, for non-SDOT users of Cameleon that is appropriate to their use of the system.	
SDOT Concurrence: Yes	Estimated Date of Completion: Q4 2021
SDOT has developed a more structured annual training program for both SDOT and non-SDOT users. We will ensure every user is trained using these new materials by Q4 2021.	
Recommendation 12: The Seattle Department of Transportation's (SDOT) Transportation Operations Center should maintain documentation of when training was completed for all Cameleon users (within and outside of SDOT).	
SDOT Concurrence: Yes	Estimated Date of Completion: Q4 2021
SDOT will maintain documentation of when training was completed for all Cameleon users.	
Recommendation 13: The Seattle Department of Transportation should work with the City Records Manager and the City Auditor to identify the appropriate retention and ensure it is listed correctly on the SDOT retention schedules so that Cameleon logs meet both the City's recordkeeping requirements and maintain availability of the logs for the City Auditor's Office to complete annual surveillance usage reviews of the CCTV technology.	
SDOT Concurrence: Yes	Estimated Date of Completion: Q3 2021
SDOT will work with the City Records Manager and the City Auditor to set a retention period for Cameleon logs as recommended.	
Recommendation 14: The Seattle Department of Transportation should rewrite Surveillance Impact Report Operational Policy 9 to clarify which logs the requirements are referring to.	
SDOT Concurrence: Yes	Estimated Date of Completion: Q3 2021
SDOT will rewrite Operational Policy #9 as recommended.	
Recommendation 15: Section 8.2.1 in the Closed-Circuit Television Camera (CCTV) Surveillance Impact Report should be revised to accurately reflect the current practice of each camera being checked once daily by Seattle Department of Transportation CCTV camera operators to ensure that it is in its home preset position.	
SDOT Concurrence: Yes	Estimated Date of Completion: Q3 2021
SDOT will revise Section 8.2.1 of the SIR to accurately reflect the daily practice of home preset positioning.	
Recommendation 16: The Seattle Department of Transportation should begin consistently documenting the rationale for its decisions about where to locate new CCTV cameras.	
SDOT Concurrence: Yes	Estimated Date of Completion: Q3 2021
SDOT will develop a SOP for consistently documenting the rationale for CCTV locations.	

Recommendation 17: To ensure that the Seattle Department of Transportation can appropriately respond to and report on complaints about misuse of surveillance technologies, it should document all complaints and concerns from all sources, including from social media.	
SDOT Concurrence: Yes	Estimated Date of Completion: Q3 2021
SDOT will develop an SOP to document concerns about the misuse of surveillance technologies from all sources.	

APPENDIX E

Numbering of Surveillance Impact Report Operational Policies

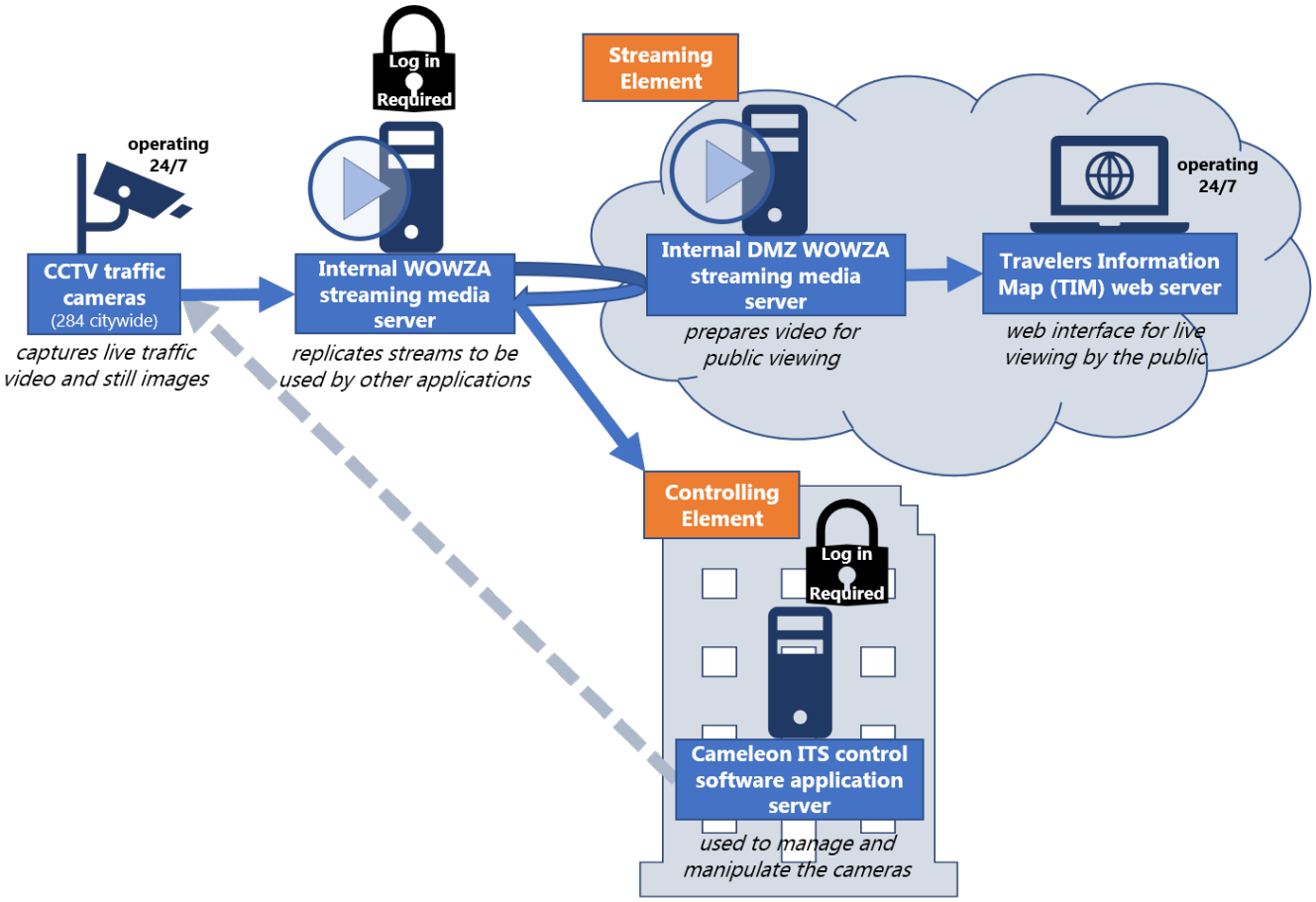
The operational policies in the adopted CCTV Surveillance Impact Report (SIR) are not numbered. Please refer to the chart below for the numbers we assigned to the operational policies in the CCTV SIR and to which we refer in this audit report. We also list the section in this audit report where we discuss and assess compliance foreach operational policy.

Assigned Operational Policy Number	Text from CCTV Surveillance Impact Report
Operational Policy 1 (Section A: Technology Use and Trends)	The SDOT CCTV System will be used to monitor general traffic conditions on public rights of way, traffic conditions after an unplanned incident, and traffic conditions impacted by a planned event.
Operational Policy 2 (Section B: Technology and Data Sharing)	The CCTV system and data shall be used only for traffic management purposes, except for when the City's Emergency Operations Center is activated to respond to an emergency or to monitor a major city-wide event, in which case the system may be used by other city personnel (e.g., Police and Fire). The system shall not be used for civil or criminal enforcement purposes.
Operational Policy 3 (Section A: Technology Use and Trends)	The CCTV System includes any dedicated video or still camera owned or operated by SDOT, mounted on a traffic pole or at an intersection, that collects data about and/or images of vehicular traffic. Cameras that detect vehicle presence and those that count and/or classify vehicles are exempted from the policies and procedures described herein.
Operational Policy 4 (Section B: Technology and Data Sharing)	SDOT only supports users of the software in the following departments or functional areas: 1. SDOT Transportation Operations Center 2. SDOT Maintenance Operations Unit Dispatch 3. SDOT Traffic Signal Shop 4. SDOT Traffic Signal Timing Engineers 5. Seattle Emergency Operations Center 6. Seattle Executive Protection Unit 7. Seattle Fire Alarm Center 8. Seattle Police Operations Center
Operational Policy 5 (Section C: Protocols for Data Management)	CCTV operators must make reasonable efforts to limit data capturing to video or still images of traffic conditions within public right of way or other publicly owned property.
Operational Policy 6 (Section C: Protocols for Data Management)	Operators may not intentionally use the CCTV cameras to discern any personally identifiable information that would enable the operators to identify a member of the public, unless doing so is necessary to allow the operator to perform a traffic management function. For any recording that does take place, the operator will record no more information than necessary for the traffic management function.

	Operators will make reasonable efforts to limit CCTV video or still images of traffic conditions.
Operational Policy 7 (Section C: Protocols for Data Management)	SDOT shall develop standard training for operation of the SDOT CCTV Traffic Camera System and handling and deletion of data collected by it in accordance with this Section and with any additional applicable SDOT policies, and only employees who have undergone such training may access or use the SDOT CCTV Traffic Camera System.
Operational Policy 8 (Section C: Protocols for Data Management)	The SDOT CCTV System will not be used to collect any data other than the following: • Live-streamed feed of current traffic conditions • Recorded video of traffic for engineering studies • Still images of traffic conditions used in training materials or included in social media
Operational Policy 9 (Section C: Protocols for Data Management)	SDOT must keep a log of all access to and operations of the CCTV, including streaming stop/start, recording dates and topics. If new equipment provides capability to log camera adjustments, SDOT will revise its procedure accordingly.
Operational Policy 10 (Section C: Protocols for Data Management)	Any City employee, whether an internal SDOT employee or other departmental user of the System, and those accessing data collected by the System, must complete training prior to using the system or accessing data collected by it.
Operational Policy 11 (Section C: Protocols for Data Management)	CCTV camera videos recorded for engineering studies will be deleted within 10 days.
Operational Policy 12 (Section C: Protocols for Data Management)	Traffic Camera video recordings used for engineering studies will be destroyed after 10 days and may be accessed only by SDOT employees.
Operational Policy 13 (Section B: Technology and Data Sharing)	The CCTV cameras will provide a 24x7publicly available livestream.
Operational Policy 14 (Section B: Technology and Data Sharing)	SDOT may disseminate live video streams over its web page, provided that users accessing the stream are notified that the system is intended to be used to monitor traffic and for no other purpose.
Operational Policy 15 (Section D: Civil Liberties Impact)	SDOT will install CCTV cameras based on street transportation volumes and locations based on gaps in travel time coverage along corridors identified in the SDOT ITS Strategic Plan.

APPENDIX F

Closed Circuit Television (CCTV) Traffic Cameras Technology



The Seattle Department of Transportation (SDOT) owns and maintains 284 Closed Circuit Television (CCTV) traffic cameras throughout Seattle. (mapping data) These cameras are powered on and providing streaming video 24 hours a day, 365 days a year.

CCTV cameras collect the following data:

- Live-streamed feed and still images of current traffic conditions
- Recorded video of traffic for engineering studies
- Still images of traffic conditions used in training materials or included in social media

CCTV cameras are installed along most major arterials, and are usually mounted on traffic poles at intersections containing traffic signals. The cameras are usually powered by the nearest traffic signal cabinet.

CCTV traffic camera data is transmitted on the following servers:

- **Internal WOWZA server**: The live video is transmitted from the physical CCTV cameras to the City's internal streaming media servers, called WOWZA. This connection occurs using SDOT's private fiber-optic ITS network. WOWZA is used to send the video streams to the DMZ WOWZA server and the Cameleon application server. Only TOC Technical Team and TOC Operators can access WOWZA.

- **Internal DMZ WOWZA server**: The DMZ WOWZA server requests live video stream data from the Internal WOWZA server, so that it can be prepared for live streaming to the Traveler Information Map via an encrypted connection.

- **Traveler Information Map web server**: This is a web interface for the public to view the live video feed from the CCTV cameras. Live streaming data and still images are transmitted from the DMZ WOWZA to the Traveler Information Map (TIM) web server.

- **Cameleon ITS Control Software application server**: The Cameleon application is used by the SDOT TOC Operators and select other City department users to access the cameras and manipulate the physical CCTV cameras, including full pan, tilt, and zoom. Camera manipulation commands travel via an encrypted connection.

Only authorized users of SDOT's Cameleon ITS control software application can remotely control the CCTV cameras, including full pan, tilt, and zoom. The TOC Technical Team manages user access, and grants access and privileges based on the role of the user. A user must have the Cameleon application installed on their computer, and they must log in with a username and password. SDOT created a hierarchy of users if two or more users wants to control a particular camera at the same time.

The TOC Technical Team can also control CCTV cameras through a built-in web interface, though this method is only used to configure new cameras, perform upgrades, or address issues. Twice daily, TOC Operators view every camera to ensure that the camera is in the correct position, or the home preset. This prevents cameras from being left in a manipulated state. TOC Operators can save video recordings from the Internal WOWZA streaming media server.

APPENDIX G

Camera Control Protocol

SDOT
Seattle Department of Transportation

SDOT Camera Control Protocol

Prior to taking control of any SDOT CCTV camera, users MUST:

1) Notify the Transportation Operations Center (TOC) staff member at (206) 684-5117 (between the hours of 6:00 am – 10:00 pm daily) or 684-5122 at all other times.

AND

2) Must comply with the RULES OF USE listed below.

USER PRIORITY:

SDOT traffic cameras are available to the public via both live feeds to the website (http://web6.seattle.gov/travelers/) and static images updated every minute. They are typically pointed in a direction, called the "home preset". Each camera will return to its home preset every five minutes of inactivity, unless it is locked by a user. Locking a camera will allow the user to maintain the camera view until it is unlocked and returned to its home preset, or a higher priority user takes control.

The SDOT TOC has the highest priority and can lock out other users (listed below) from taking control of the camera. When the CCTV camera is locked by the SDOT TOC, no other user has the ability to move it. If lower level users have a need of any SDOT CCTV camera, that user must contact the SDOT TOC (as listed above) and the CCTV may be released for their use (depending on the current use versus the requested use). NOTE: Control will be returned to the TOC at such time that an incident of a higher priority as determined by the SDOT TOC presents itself. The TOC will attempt to notify the lower level user.

USERS INCLUDE:

- Mayor's Office
- SDOT Charles Street Dispatch
- EOC
- SFD
- SPD/SPOC

RULES OF USE

Closed Circuit Television (CCTV) cameras implemented by SDOT are for the purposes of traffic management, incident management and response, and public information. CCTV cameras and images are used in a manner consistent with the public's expectation of privacy, while serving their function as a traffic management and traveler information tool.

In order to implement these policies, SDOT has created the following rules:

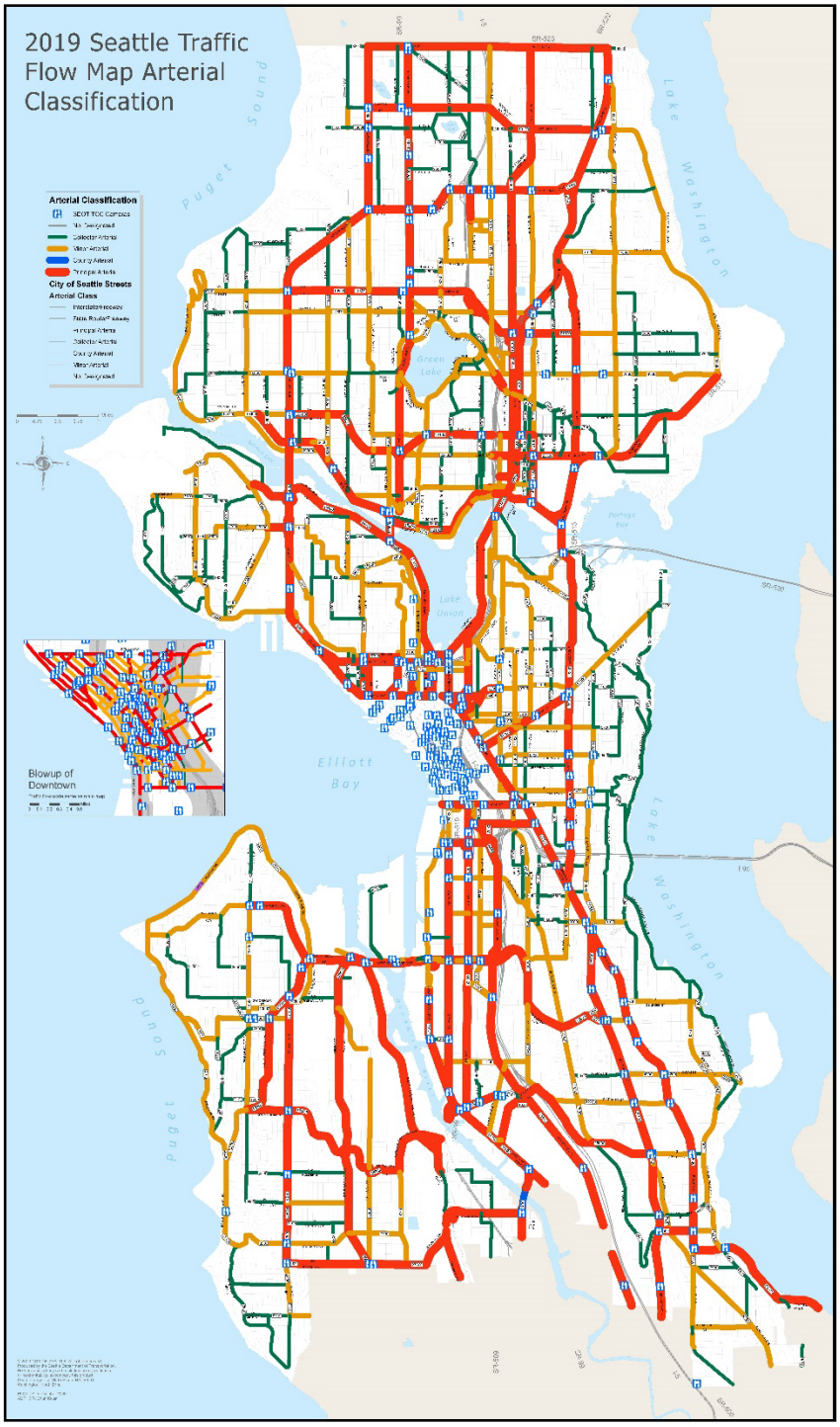
- CCTVs shall be used to monitor conditions on SDOT-owned roadways, and shall not be used to monitor conditions on the sidewalk or on private property.
- Operator shall not use the CCTV cameras to zoom in close enough to discern any information that would enable the operators to identify a member of the public, including, without limitation, license plate numbers, unless doing so is absolutely necessary to allow the operator to perform a vital component of their jobs.
- Should it be necessary to view personally-identifiable information, the operator shall terminate any dissemination of the CCTV feed to the general public prior to viewing such information, and shall not resume dissemination until personally-identifiable information is no

longer visible.

- Video images will not be recorded, except for compelling traffic operational needs. If they are recorded, any such recordings will be destroyed immediately after use. Recordings shall not be stored or disseminated.
- Subject to these limitations, SDOT may disseminate images or video streams over its web page.

APPENDIX H

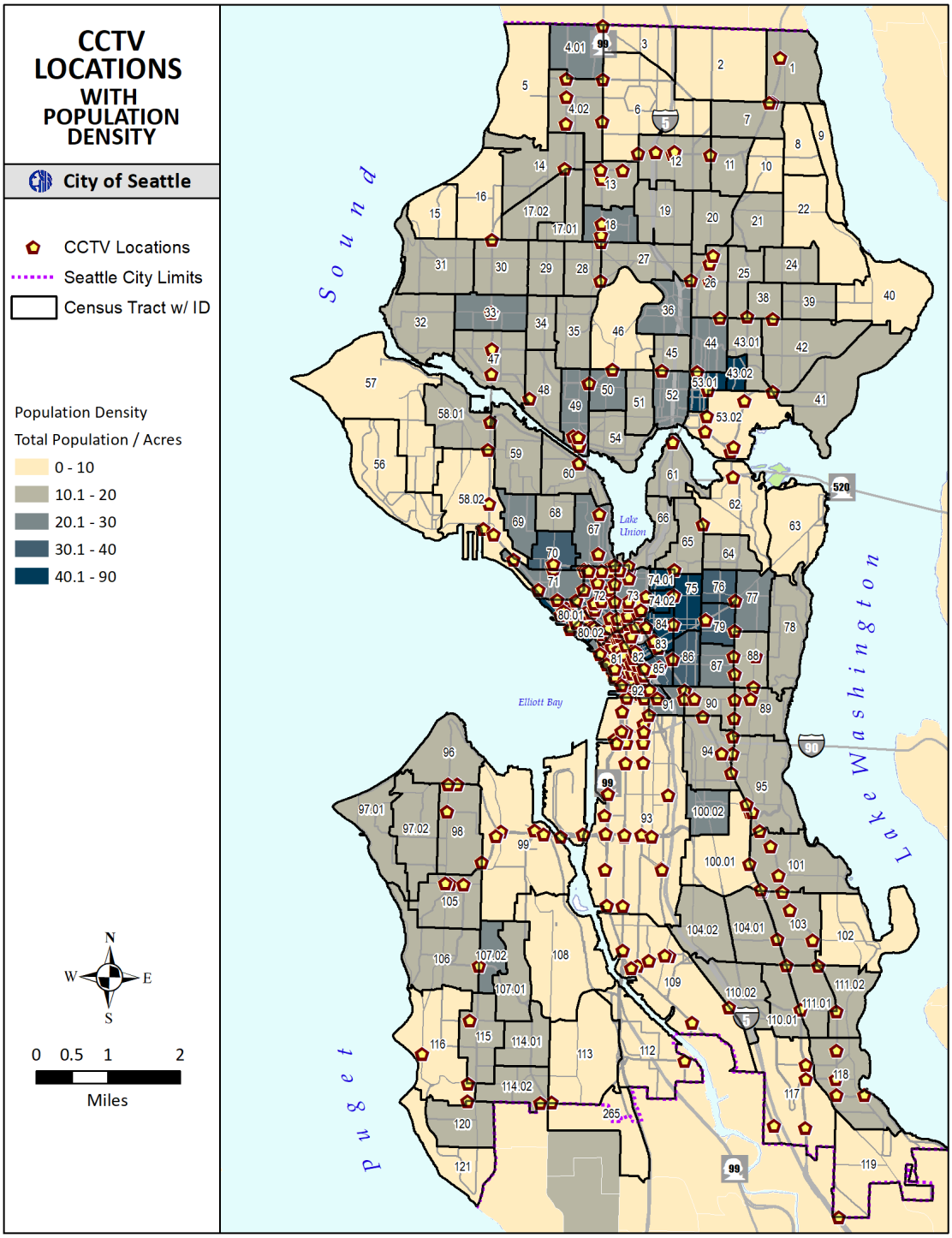
2019 Seattle Traffic Flow Map



Source: Seattle Department of Transportation.

APPENDIX I

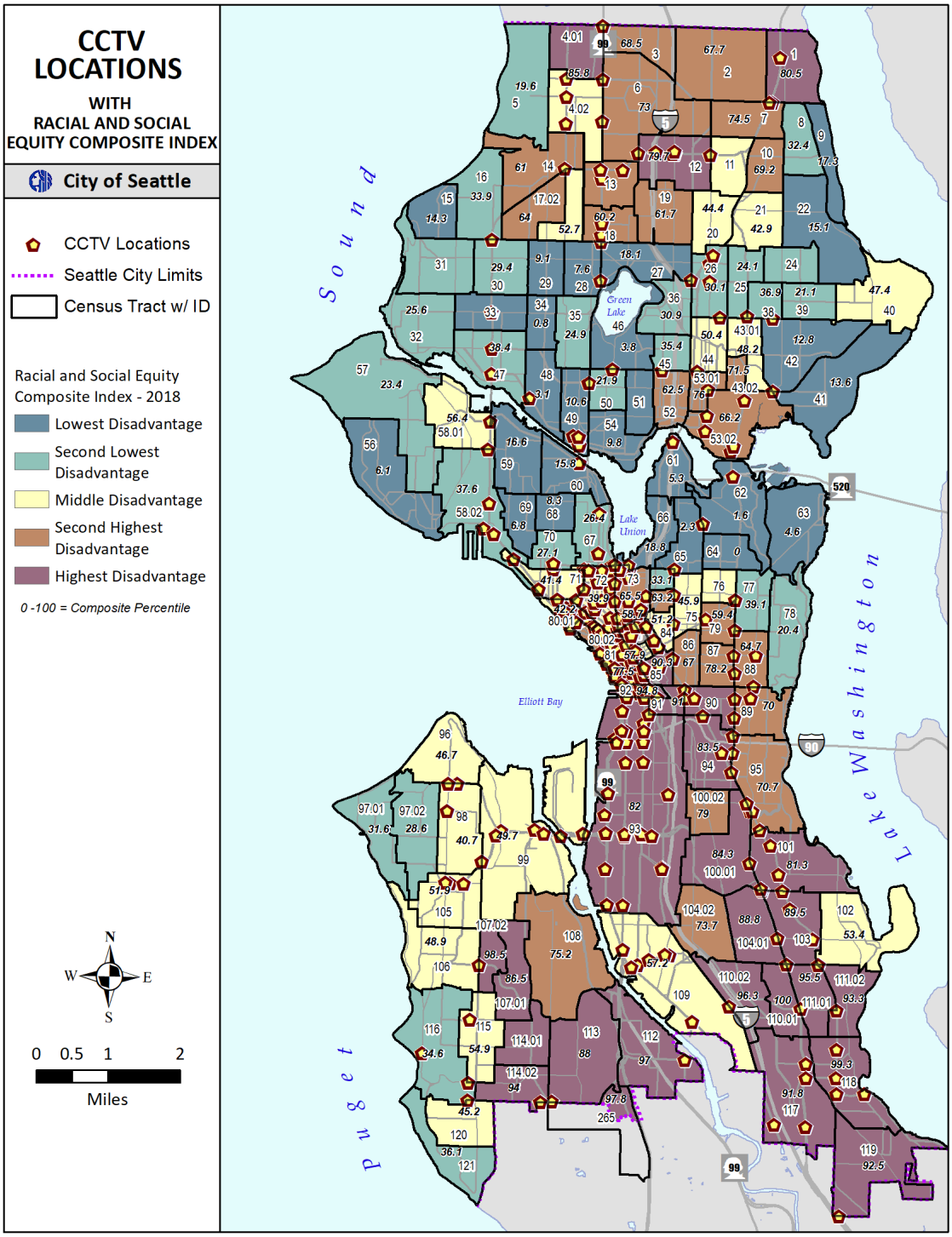
Population Density



Source: Seattle Information Technology Department analysis of Seattle Department of Transportation data.

APPENDIX J

Race and Social Equity Composite Index



Source: Seattle Information Technology Department analysis of Seattle Department of Transportation data.

APPENDIX K

Acknowledgements

The Office of City Auditor would like to thank staff from the following City departments for their cooperation on this audit and responsiveness to requests for information, documents, and data:

- SDOT Transportation Operations Center (TOC)
- SDOT Finance and Administration Division
- SDOT Project Development Division
- Legislative City Clerk, Information Technology
- Finance and Administrative Services, Customer Services Division
- Seattle Information Technology Department, GIS Products and Services
- Seattle Information Technology Department, Privacy Team
- Seattle Information Technology Department, Cybersecurity/Risk Management
- Office of Planning & Community Development, Citywide Initiatives
- Seattle Police Department
- Office of Emergency Management

We would like to thank the Seattle Information Technology Department, GIS Products and Services for providing GIS mapping and demographic analysis.

We would also like to thank the following parties from outside the City of Seattle:

- ACLU of Washington
- A citizen advocate for surveillance technology concerns

APPENDIX L

Seattle Office of City Auditor Mission, Background, and Quality Assurance

Our Mission:
To help the City of Seattle achieve honest, efficient management and full accountability throughout City government. We serve the public interest by providing the City Council, Mayor and City department heads with accurate information, unbiased analysis, and objective recommendations on how best to use public resources in support of the well-being of Seattle residents.

Background:
Seattle voters established our office by a 1991 amendment to the City Charter. The office is an independent department within the legislative branch of City government. The City Auditor reports to the City Council and has a four-year term to ensure her/his independence in deciding what work the office should perform and reporting the results of this work. The Office of City Auditor conducts performance audits and non-audit projects covering City of Seattle programs, departments, grants, and contracts. The City Auditor's goal is to ensure that the City of Seattle is run as effectively, efficiently, and equitably as possible in compliance with applicable laws and regulations.

How We Ensure Quality:
The office's work is performed in accordance with the Government Auditing Standards issued by the Comptroller General of the United States. These standards provide guidelines for audit planning, fieldwork, quality control systems, staff training, and reporting of results. In addition, the standards require that external auditors periodically review our office's policies, procedures, and activities to ensure that we adhere to these professional standards.

Seattle Office of City Auditor
700 Fifth Avenue, Suite 2410
Seattle WA 98124-4729
Ph: 206-233-3801
www.seattle.gov/cityauditor