



# Seattle Office of Inspector General

## Surveillance Technology Usage Review: Computer-Aided Dispatch (2021)

---

As Required by Seattle Municipal Code 14.18.060

April 28, 2023

Office of Inspector General  
City of Seattle  
PO Box 94764  
Seattle, WA 98124-7064  
[oig@seattle.gov](mailto:oig@seattle.gov)  
(206) 684-3663

## Foreword from the Inspector General

Enclosed is OIG's first Annual Surveillance Usage Review on the use of Computer-Aided Dispatch (CAD) by the Seattle Police Department (SPD). This review was performed pursuant to Seattle Municipal Code 14.18.060, which specifies that OIG conduct annual reviews of SPD's use of Surveillance Technologies. CAD is one of sixteen SPD Surveillance Technologies currently approved by City Council.

OIG contracted with cybersecurity firm Critical Insight to conduct this review, and we thank them for their work, as well as their ongoing partnership in overseeing SPD's use of approved Surveillance Technologies.

Throughout this process, OIG directed and reviewed the work of Critical Insight. OIG also facilitated stakeholder feedback from SPD, the American Civil Liberties Union, and City Council staff. We appreciate the time and effort these stakeholders devoted to this review. These consultations and perspectives helped to ensure the work was thorough and inclusive, and that our conclusions and recommendations are based on the most complete information available.

In performing this review annually, OIG will continue to engage with SPD and other stakeholders to ensure responsiveness to community concerns and innovate in the area of evaluating how SPD uses Surveillance Technologies to further public safety while protecting the rights of individuals in our community.



# Critical Insight

## CITY OF SEATTLE SURVEILLANCE TECHNOLOGY REVIEW COMPUTER-AIDED DISPATCH (CAD)

SOW-2022-271

APRIL 28, 2023

### **Notice**

Critical Insight has made every reasonable attempt to ensure that the information contained within this statement of work is correct, current and properly sets forth the requirements as have been determined to date. The parties acknowledge and agree that the other party assumes no responsibility for errors that may be contained in or for misinterpretations that readers may infer from this document.

### **Trademark Notice**

2023 Critical Insight, Inc. dba CI Security. All Rights Reserved, CI Security®, Critical Insight™, the Critical Insight and Kraken logos and other trademarks, service marks, and designs are registered or unregistered trademarks of Critical Insight in the United States and in foreign countries.

**© Copyright 2023 Critical Insight, Inc.**

## Table of Contents

---




<b>Executive Summary .....</b>	<b>4</b>
<b>Summary of Assessments and Recommendations Related to SMC 14.18.060 .....</b>	<b>4</b>
<b>Technology Description .....</b>	<b>6</b>
<b>Purpose and Objectives.....</b>	<b>7</b>
<b>A. Surveillance Technology Usage.....</b>	<b>9</b>
<b>B. Data Sharing with External Entities .....</b>	<b>11</b>
<b>C. Data Management and Safeguarding of Individual Information.....</b>	<b>12</b>
<b>Data Retention .....</b>	<b>12</b>
<b>Safeguarding of Individual Information .....</b>	<b>13</b>
<b>D. Impact on Civil Liberties and Disproportionate Effects on Disadvantaged Populations .....</b>	<b>14</b>
<b>Impact on Civil Liberties .....</b>	<b>14</b>
<b>Disproportionate Effects on Disadvantaged Populations.....</b>	<b>14</b>
<b>E. Complaints, Concerns and Other Assessments.....</b>	<b>16</b>
<b>Office of Police Accountability (OPA) Complaints.....</b>	<b>16</b>
<b>Customer Service Bureau Complaints .....</b>	<b>16</b>
<b>Internal Audits or Assessments .....</b>	<b>16</b>
<b>F. Cost Auditing.....</b>	<b>16</b>




## Executive Summary

---

This Executive Summary highlights major findings and recommendations pertaining to the six elements of SMC 14.18.060, which structures OIG’s review. The summary below lists our significant audit results associated with SMC 14.18.060.

### Summary of Assessments and Recommendations Related to SMC 14.18.060

14.18.060 Provision	Compliance Determination	Auditor’s Finding	Recommendations
A. How surveillance technology has been used, usage frequency, and whether usage patterns have changed.	<b>Yes</b> 	SPD already provides public data to explain the frequency and type of CAD usage. Patterns or changes in use are directly related to the number of incidents reported or identified.	
B. How often surveillance technology or its data are shared with other entities, including government agencies.	<b>Yes</b> 	External entities must request CAD records through the Criminal Records Unit or the Public Records Request Center. CAD records are requested daily. Given the volume and search limitations, it was not feasible for this review to determine a number of records provided to external entities.	
C. How well data management protocols are safeguarding individual (personal) information.	<b>Needs Work</b> 	Neither Seattle IT nor SPD are conducting regular access audits of Mark43 or CAD, and access to these systems is not monitored to detect patterns of access that could indicate account compromise or unauthorized sharing of accounts.	No recommendations toward this finding at this time, as the system, policies, and processes addressed in this section are broader than the scope of this technology review. OIG will continue to monitor this concern and explore potential follow-up work to address the systemwide concerns.

14.18.060 Provision	Compliance Determination	Auditor's Finding	Recommendations
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.	<b>Yes</b> 	CAD technology itself does not present significant risk for disproportionate use as it only reflects community calls and SPD responses. Personally Identifiable Information may be included in CAD, however PII is used to inform appropriate law-enforcement responses. The retention and security of such data is a greater determinate of civil liberties concerns.	
E. A summary of any complaints or concerns about the surveillance technology and results of internal audits or assessments of code compliance.	<b>Yes</b> 	Our review found no known complaints related to the use of CAD.	
F. Total annual costs for use of surveillance technology, including personnel and other ongoing costs.	<b>Yes</b> 	The annual cost for CAD in 2021 is in line with the cost stated in the 2019 Surveillance Impact Report.	

## Technology Description

---

The Seattle Police Department (SPD) uses the Computer-Aided Dispatch (CAD) system to coordinate and document, in real-time, requests for police service and SPD's response to those requests. The technology is used by 9-1-1 call takers to document information reported by a 9-1-1 caller and then assists 9-1-1 dispatchers with prioritizing emergency calls and assigning appropriate police resources to incidents. CAD events include criminal and non-criminal activity and may be generated either by the community (such as members of the public calling 9-1-1) or by an officer (such as when an officer observes a crime in progress). As such, the use of CAD and any resulting patterns reflect the activities of the department more than the technology itself. In the Surveillance Impact Report (SIR) for this technology, SPD estimated that 250,000 CAD events are created from the approximately 900,000 calls received by the 9-1-1 center annually, and approximately 135,000 additional CAD events are created annually from patrol officers viewing incidents, such as traffic violations.

Developed in the 1960s, CAD systems are used by virtually all modern police departments. Computer-Aided Dispatch increases efficiencies in police-related emergency response. CAD also provides information that allows SPD to allocate patrol resources effectively while reducing response times. CAD is the real-time record-keeping system for officers' response to calls for service, thereby documenting SPD's actions related to each of those requests in an organized and reportable method.

The CAD system automatically receives the telephone number, name attributed to the telephone number (if available), the type of telephone service (cellular, landline, or VOIP phone), and location of the caller (if available) from the West VIPER telephone system for calls placed to 9-1-1. Non-emergency calls and associated phone numbers are not automatically entered into CAD. If the call is determined to be a request for police services, call takers and dispatchers then manually enter additional information into CAD, such as the nature of the emergency, and create a CAD event to facilitate a police response. Call takers and dispatchers may add supplemental information into CAD regarding scene safety, descriptions of individuals, vehicles, and premises. Much of the privacy-sensitive information entered into CAD comes from 9-1-1 or non-emergency callers, officers, or dispatchers who input information into the CAD system when responding to a call.



All information and data entered into CAD are viewable and retrievable. Some information from one call may be used for subsequent calls at the same location or involving the same individuals.

## Purpose and Objectives

---

The purpose of this document is to communicate the findings of an analysis of the SIR and associated departmental policies and processes for SPD's use of the CAD system to coordinate the dispatch of SPD assets.

This analysis was conducted by Critical Insight consultants at the request of the Office of the Inspector General for Public Safety (OIG) at the City of Seattle under City Ordinance 125376, under Chapter 14.18.060, which requires an annual review of actual usage of surveillance technologies by the Seattle Police Department. Per Ordinance 125376, this review is required to include, but is not 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, including, for SPD, an examination of whether deployments are pursuant to warrants or not and how SPD's surveillance technology is used to analyze patterns to predict suspect, individual, or group-affiliation behavior;
- 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.

In the course of this review, consultants reviewed the information disclosed in the SIR, as well as Seattle Police Department policy relating to evidence handling, video

surveillance and bias-free policing, and reviewed data showing the number and types of incidents handled during calendar year 2021 both in aggregate and broken down to the neighborhood level. This review also included a survey of concerns raised by the Privacy and Civil Liberties Assessment and Public Comment sections of the SIR.

This report will highlight risks discovered by Critical Insight consultants in the following areas, and give recommendations on how to remediate those risks:

- Is the description of the technology in the SIR complete and accurate?
- Is there a clear usage and data management policy or policies in place?
- Does the SIR and/or policy describe how and when the surveillance technology will be deployed, and by whom?
- How and where will data gathered by this surveillance technology be stored?
- How long will the data be retained?
  - What process is used to destroy data that are no longer being retained?
- How is access to the data secured?
  - How is unauthorized access prevented?
  - What access reviews are being performed?
- How are data shared outside of the department, and how is sharing or access to those data monitored and audited?
- Are there any auditability concerns about the technology, its cost, and its usage in general?
  - Example: Instances where access authorization cannot be reviewed because log data is not available.
  - Example: Instances of the use of a particular surveillance technology not being tagged properly in case notes.

## A. Surveillance Technology Usage

SPD reports that 331,613 CAD events were recorded during calendar year 2021. Of these, 261,579 events (78.88%) were generated by the community, 69,776 (21.04%) were generated by officers in the field, and 258 events (0.07%) in CAD did not have an identified source.

SPD provides an online, publicly accessible dashboard for CAD events. Data in this report are sourced from that dashboard.<sup>1</sup>

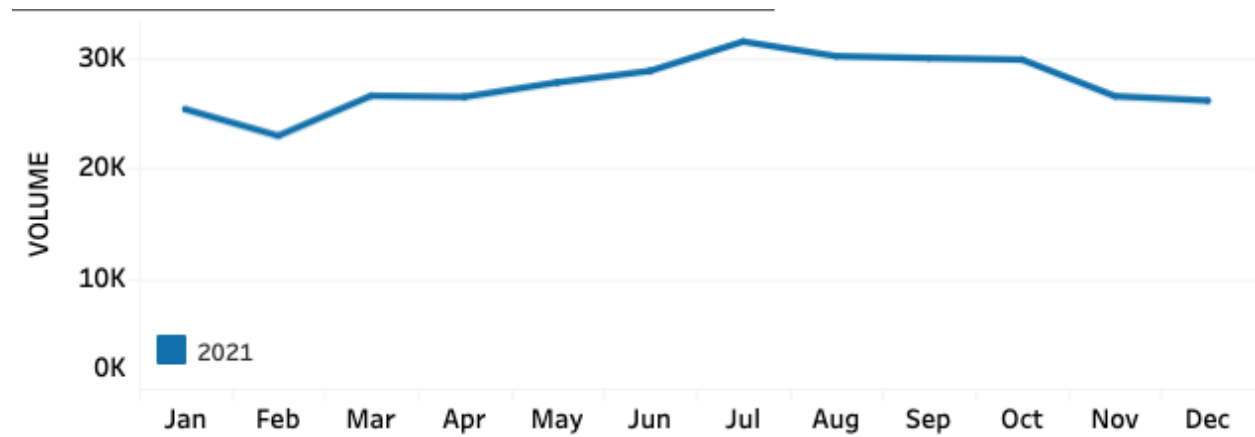
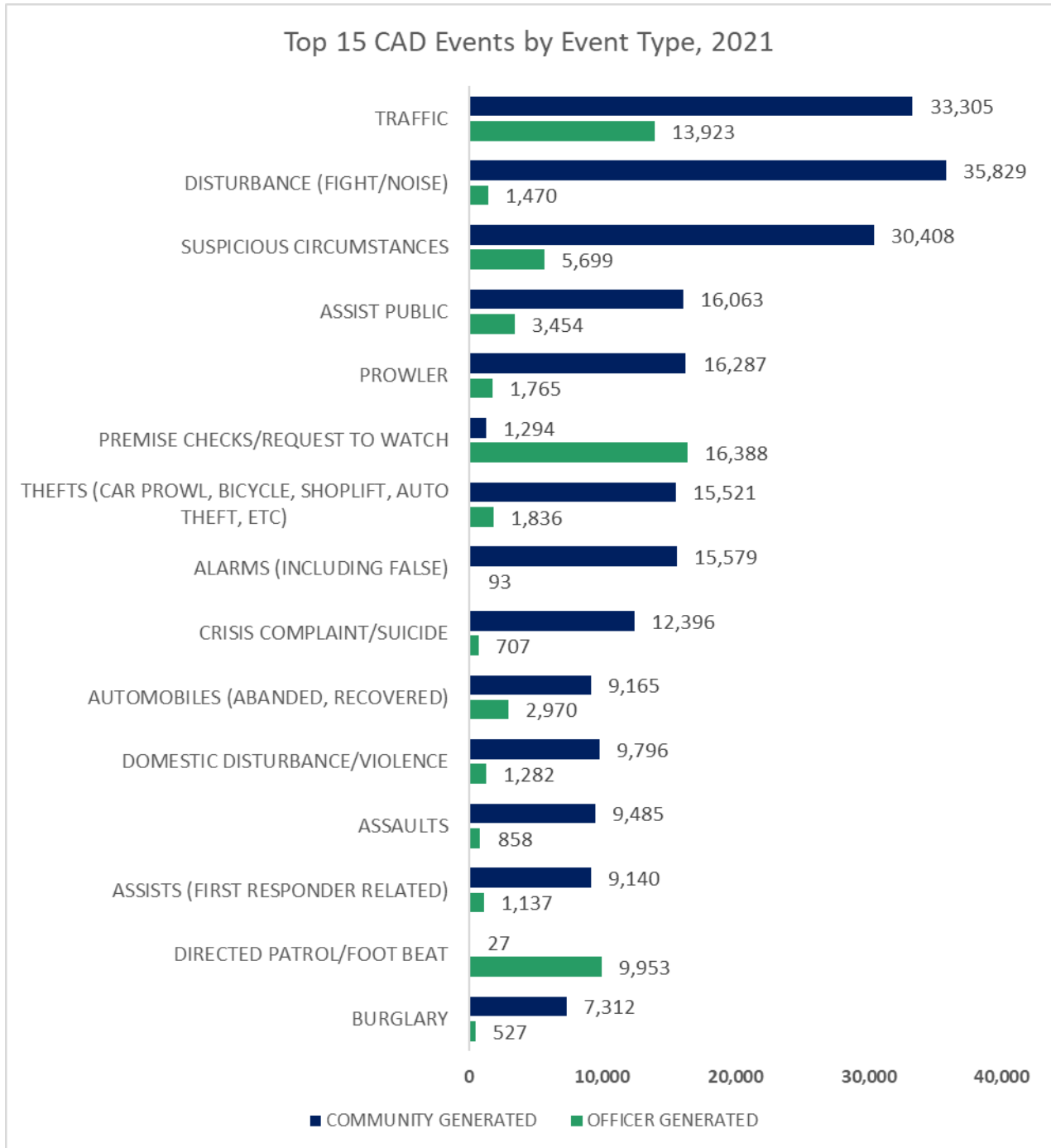


Figure 1 - Monthly CAD Event Volume in 2021

<sup>1</sup> <https://www.seattle.gov/police/information-and-data/data/computer-aided-dispatch-dashboard>



**Figure 2 - Distribution of CAD Event Types in 2021**

Note that CAD events may change as information is discovered during an investigation. CAD events as reported in this figure represent the final nature of the event and have been grouped by SPD for reporting purposes.

## B. Data Sharing with External Entities

---

The SIR states that CAD data may be shared outside of SPD with the following agencies, entities, or individuals within legal guidelines or as required by law:

- Seattle City Attorney's Office
- King County Prosecuting Attorney's Office
- King County Department of Public Defense
- Private Defense Attorneys
- Seattle Municipal Court
- King County Superior Court
- Similar entities where prosecution is in Federal or other State jurisdictions
- Members of the public pursuant to the Washington Public Records Act, Chapter 42.56 RCW

Per SPD Policy 12.080, requests for CAD data from external entities such as other City departments, law enforcement agencies, and insurance companies should be submitted through the Crime Records Unit. However, SPD personnel explained that requests from external entities are also submitted through SPD's Public Records Request Center. Per SPD, CAD data are never given to an outside agency without first being imported into Mark43, and at no point do external entities have direct access to reports in CAD or Mark43.

SPD reports that data from CAD are requested and shared with external entities and individuals daily. Due to the volume of requests and limits in filtering searches, it was not feasible to generate an accurate assessment of the number of CAD records released to external entities or individual members of the public.

## C. Data Management and Safeguarding of Individual Information

---

When an individual calls 9-1-1, the telephone number they are calling from, the location they are calling from, the name associated with the phone number (if available from the phone company), and the type of telephone service (landline, cell phone, VOIP phone) are provided by the West VIPER telephone system and automatically entered into CAD. Additionally, 9-1-1 dispatchers may include private information about a subject, such as a warrant check or vehicle registration status, at the request of responding SPD officers. Although community members raised few complaints or concerns about the use of CAD in the creation of the SIR, most comments cited data storage, security, and retention concerns. These concerns are explored below, including the extent to which current SPD policies deter, detect, and record improper access to and activities in the CAD and Mark43 systems.

### Data Retention

In a memo to the Seattle City Council dated April 24, 2019, an SPD Deputy Chief stated that “Data entered into SPD’s CAD system is retained indefinitely on Seattle IT managed servers dedicated to the CAD system. No data is deleted; however, updates are made as necessary to records.” Additionally, Section 6.6 of the SIR states that “SPD cannot delete any information in CAD. Updates to information may be added to individual CAD events by SPD personnel with access to CAD.”<sup>2</sup>

A subset of CAD data, including identifying information (date, time and location of the event, descriptions of suspects, names of responding officers, name of the person reporting the event, and names of involved persons if known) are migrated into SPD’s Records Management System (RMS), Mark43. According to SPD personnel, records in Mark43 are retained indefinitely. Sensitive personally identifying data entered into CAD are retained indefinitely in both systems.

The current policy of indefinite retention does not conflict with the retention periods set by the Washington State Law Enforcement Records Retention Schedule, as those retention periods only establish minimums.

---

<sup>2</sup> Section 7.1 of the SIR provides that SPD retains CAD data that is not case-specific for 90 days. SPD identified that this was an error, and all data is currently retained.

## Safeguarding of Individual Information

In 2022, the FBI audited SPD's overall Criminal Justice Information Services (CJIS) and noted violations of CJIS security policy with respect to Mark43 and CAD. The following sections give the text of each relevant finding as well as our understanding of the current status of remediation.

### Auditing of Access and Activity Logs

*CJIS Security Policy*, Version 5.9, June 2020, 5.4 Policy Area 4: Auditing and Accountability, pp. 27-28

*Policy Finding: **OUT***

***Ensure logs for Mark 43 are reviewed weekly and retained for a minimum of one year.***

***Ensure Oracle logs for the Reposit (Versaterm Legacy RMS data pool) and Composit (Versaterm CAD data pool) are reviewed at least weekly.***

The FBI CJIS security policy requires that event logs of CJI databases such as Mark43 and CAD be scanned at least weekly in order to mitigate threats of compromised accounts or users exploiting access to sensitive information. Industry best practice is to perform this scan on a continuous basis using a combination of automated tools and human analysts.

From interviewing SPD personnel, we understand that the City is in the process of exploring how Mark43 access could be reviewed in real time by the City's Security Operations Center. This appears to be a capability that Mark43 does not currently provide. SPD is working with Mark43 to address these security needs; however, Mark43 is not CJIS-compliant in this regard until these security issues have been addressed.

The second finding states that Oracle database server logs are not being reviewed weekly by the City. The CAD logs are retained because they are generated by on-premises systems, whereas Mark43 is a Software-as-a-Service (SAAS) application whose log storage Seattle IT does not control. Unlike Mark43, there does not appear to be a limitation within the CAD system impeding the review and retention of logs.

Critical Insight is not making recommendations at this time, as the systems, policies, and processes addressed in this section are broader than the scope of this

technology review. OIG will continue to monitor this concern and explore potential follow-up work to address the systemwide concerns.

## D. Impact on Civil Liberties and Disproportionate Effects on Disadvantaged Populations

---

### Impact on Civil Liberties

As noted in Section C of this report, personally identifiable information (PII) is regularly captured in CAD. Examples may include the telephone number an individual is calling from, the location they are calling from, and the name associated with the phone number. PII may also be entered manually by personnel responding to a call. The collection and sharing of PII through CAD are generally necessary to provide responding officers with timely and accurate information about the people they are encountering; however, PII collection and sharing do increase the risk of negative impacts for the owners of that PII if data are not adequately protected.<sup>3</sup>

Warrants are not required to collect information in CAD, and while CAD and Mark43 may contain a significant record of a given individual or groups' interactions with SPD, such records are unlikely to be useful in predicting individual or group behaviors.

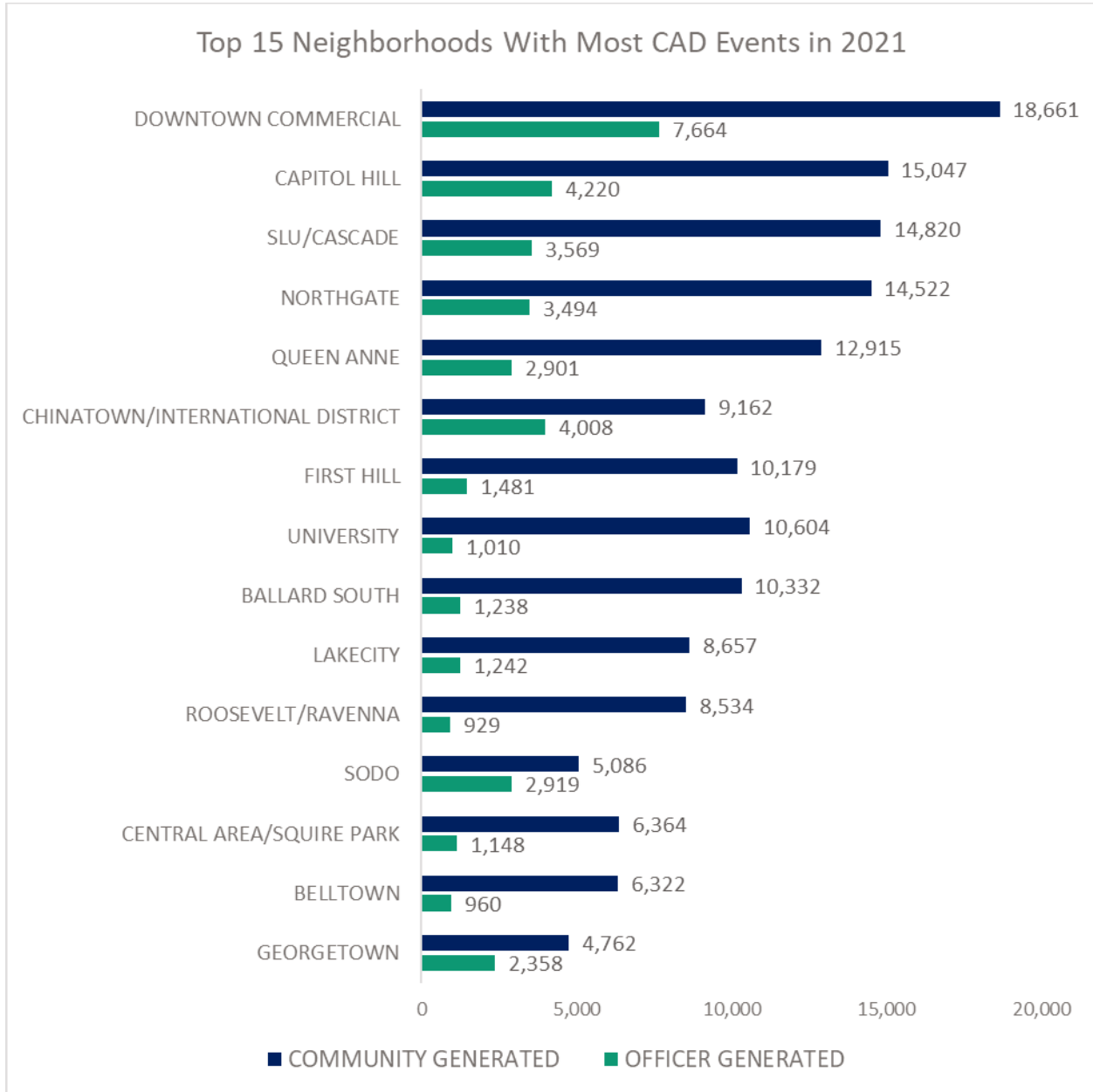
### Disproportionate Effects on Disadvantaged Populations

The CAD system documents information provided by individuals involved in events or directly observed by SPD personnel. As such, the CAD technology itself is unlikely to carry potential for disproportionate effects on disadvantaged populations. Provided these limitations, Figure 3 below highlights the neighborhoods in which the most CAD events occurred in 2021. Significant variations exist in the overall volume of CAD events between neighborhoods, as well as ratios between officer-initiated and community-initiated calls. For example, approximately 36% of CAD events in SODO were initiated by officers, whereas 9% of events in the University District were initiated by officers. These differences may reflect how SPD officers are deployed or the different types of events happening in different neighborhoods. A broad analysis of call responses and deployments would need to be performed to understand these differences; however, such an analysis is not within the scope of this technology review.

---

<sup>3</sup> Section C of this report discussed the security and retention of CAD data.





**Figure 3 – Top 15 Neighborhoods with Most CAD Events in 2021**

## E. Complaints, Concerns and Other Assessments

---

### Office of Police Accountability (OPA) Complaints

No complaints from 2021 submitted to OPA regarding the CAD surveillance technology were found.

### Customer Service Bureau Complaints

No relevant complaints or concerns from 2021 submitted to the City of Seattle Customer Service Bureau were found.

### Internal Audits or Assessments

According to SPD's Audit, Policy, and Research Section, no internal audits or assessments have been conducted on this technology.

## F. Cost Auditing

---

Based on information provided by Seattle IT, the total annual cost paid by the city in 2021 for the Versaterm CAD technology was \$338,739.35. This amount is slightly higher than the annual maintenance and licensing cost of \$333,757.00 that was provided in the 2019 SIR.

Personnel costs were not assessed as it is not feasible to accurately identify the costs associated with Community Safety and Communications Center and SPD personnel who operate and maintain this technology,



April 25, 2023

Inspector General Lisa Judge  
Office of the Inspector General

Dear Inspector General Judge:

Thank you for providing the Seattle Police Department with an opportunity to review and respond to the Office of the Inspector General's Surveillance Technology Review of Computer-Aided Dispatch (SOW-2022-271). Recognizing that there are not formal recommendations offered at part of the review, I nevertheless wanted to correct the record on the matter of data retention.

The Data Retention section states:

"A subset of CAD data, including identifying information (date, time and location of the event, descriptions of suspects, names of responding officers, name of the person reporting the event, and names of involved persons if known) are migrated into SPD's Records Management System (RMS), Mark43. According to SPD personnel, records in Mark43 are retained indefinitely. Sensitive personally identifying data entered into CAD are retained indefinitely in both systems." (p. 13)

Only part of the listed data is imported into Mark43 (example below). No suspect, reporting party, or involved person's data is migrated into Mark43 from CAD. Sensitive, personally identifying data can be stored in both CAD and Mark43, but only if the data is manually added to Mark43 during the completion of a report. It is not migrated automatically.

Report Number

**CAD EVENT INFO**

---

CAD Event #: 23000106952  
Event Time: Apr 20, 2023 20:14 - 20:23  
Primary Units: SUV2-DX  
Primary Officers: DRIVER 2 SOBERING UNIT #L002,  
Address of Event: 15 AV S & S BAYVIEW ST SEATTLE, WA 98144 UNITED STATES

**REPORT NUMBER 2023-106952 REPORTS**

---

The Safeguarding of Individual Information states:

"The second finding states that Oracle database server logs are not being reviewed weekly by the City. The CAD logs are retained because they are generated by on-premises systems, whereas Mark43 is a Software-as-a-Service (SAAS) application whose log storage Seattle IT does not control. Unlike Mark43, there does not appear to be a limitation within the CAD system impeding the review and retention of logs." (p.14)

While this finding was initially true, we were able to address it once we confirmed the logs were reviewed weekly. The ITD contact participating in the audit couldn't say with full confidence at the time of the audit. Once the responsible IT personnel were contacted, we were able to confirm that IT was in fact monitoring the logs and we were able to close that compliance issue. The only compliance issue remaining from the audit is the event logs for Mark43 and the company will be presenting its solution this week or next.

I continue to appreciate our work together to make Seattle a safer and more equitable city.

Sincerely,

A handwritten signature in black ink, appearing to read 'A. Diaz', with a stylized flourish at the end.

Adrian Z. Diaz  
Chief of Police

## **NON-AUDIT STATEMENT**

This review was not conducted under Generally Accepted Government Auditing Standards. However, OIG has reviewed the work of Critical Insight to provide reasonable assurance that evidence used in this review was sufficient and appropriate.