



# Seattle Office of Inspector General

## Surveillance Technology Usage Review: 9-1-1 Logging Recorder (2021 and 2022)

---

As Required by Seattle Municipal Code 14.18.060

September 29, 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

The following is OIG's first Surveillance Usage Review on the use of the "9-1-1 Logging Recorder" by the Community Safety and Communications Center (CSCC). This review was performed pursuant to Seattle Municipal Code 14.18.060, which requires OIG to conduct annual reviews of SPD's use of Surveillance Technologies. Although this technology was transferred out of SPD in 2021, OIG retains oversight responsibility, as information collected through it is regularly provided to SPD.

OIG contracted with a cybersecurity firm, Critical Insight, to conduct this review. OIG also facilitated stakeholder feedback from the CSCC and the American Civil Liberties Union. 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 were based on the most complete information available.



# Critical Insight

## CITY OF SEATTLE SURVEILLANCE TECHNOLOGY REVIEW 9-1-1 LOGGING RECORDER

SOW-2022-347

SEPTEMBER 29, 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><i>Executive Summary</i></b> .....	<b>4</b>
<b><i>Technology Description</i></b> .....	<b>6</b>
<b><i>Purpose and Objectives</i></b> .....	<b>6</b>
<b><i>A. Surveillance Technology Usage</i></b> .....	<b>7</b>
<b><i>B. Data Sharing with External Partners and Other Entities</i></b> .....	<b>7</b>
<b><i>C. Data Management and Safeguarding of Individual Information</i></b> .....	<b>9</b>
<b><i>D. Impact on Civil Liberties and Disproportionate Effects on Disadvantaged Populations</i></b> .....	<b>10</b>
<b><i>E. Complaints, Concerns and Other Assessments</i></b> .....	<b>11</b>
<b><i>F. Cost Auditing</i></b> .....	<b>11</b>

## Executive Summary

The summary below highlights significant audit findings and recommendations regarding compliance with SMC 14.18.060.

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

14.18.060 Provision	Compliance Determination	Auditor's Assessment	Recommendations
A. How surveillance technology has been used, usage frequency, and whether usage patterns have changed.	<b>Yes</b> 	Use of the 9-1-1 Logging Recorder software is consistent with the purpose and usage described in the Surveillance Impact Report (SIR).	
B. How often surveillance technology or its data is shared with other entities, including government agencies.	<b>Yes</b> 	In 2021 and 2022, Community Safety Communications Center (CSCC) and SPD responded to approximately 20,000 data sharing requests pertaining to call audio and/or metadata retained by the 9-1-1 Logging Recorder. Records of these sharing requests are highly detailed and tracked to entities outlined in the SIR.	
C. How well data management protocols are safeguarding individual (personal) information.	<b>Needs Work</b> 	While the records kept are very detailed and helpful for auditing purposes, they are not currently documented and formalized as an official procedure.	<b>Recommendation 1:</b> CSCC should formalize current recordkeeping practices as written procedures.
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> 	There is no evidence that voice stress or voice recognition analysis is currently being performed on 9-1-1 call recordings	

14.18.060 Provision	Compliance Determination	Auditor's Assessment	Recommendations
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> 	There were no known complaints related to the use of this technology during the review period.	
F. Total annual costs for use of surveillance technology, including personnel and other ongoing costs.	<b>Yes</b> 	The cost was \$49,199.18 in 2021 and \$51,717.91 in 2022 for renewal and maintenance.	

## Technology Description

---

The NICE Systems 9-1-1 Logging Recorder is an application that automatically records 9-1-1 and non-emergency telephone calls and police radio traffic for evidentiary and public disclosure purposes. The NICE Systems 9-1-1 Logging Recorder is maintained “on-premises”, meaning the application and its stored recordings are maintained in the SPD section of the City of Seattle datacenter.

## Purpose and Objectives

---

This analysis was conducted by Critical Insight consultants at the request of the Seattle Office of the Inspector General for Public Safety pursuant to City Ordinance 125376, Chapter 14.18.060. Per the Ordinance, this review must 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;
- 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.

In this review, consultants reviewed the information disclosed in the SIR, and conducted an on-site assessment of CSCC procedures related to this technology.

This report will highlight risks ascertained by Critical Insight consultants using the criteria listed below, and give recommendations to remedy associated 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 it 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?

## A. Surveillance Technology Usage

---

Audio recordings of 9-1-1 calls and police radio traffic can provide critical evidence to officers, detectives, prosecutors, and oversight entities. These recordings also provide transparency and accountability, as they record in real time the interactions between 9-1-1 call takers and callers, and the radio traffic among 9-1-1 dispatchers and police officers.

The NICE system also supports the CSCC's mission of quickly determining the nature of the call and getting the necessary assistance as quickly as possible with high quality, consistent, and professional services.

## B. Data Sharing with External Partners and Other Entities

---

Recordings are provided to external agencies on evidence-grade DVDs. All requests for recordings from external entities are logged with the General Offense number associated with the request, as well as the name and agency of the requestor, the priority level of the request, and the date the request was made. Most requests for copies of recordings are from the City Attorney's office and are typically received via email.

Data Origins	Shareable Data	Recipients of Data Shared
- 9-1-1 calls - calls to SPD's published non-emergency line - the nonpublished, ten-digit direct line to SPD dispatch	- call audio - phone number - start/stop time of call - duration of call - staff position of call taker	- other law enforcement - attorneys/courts - insurance companies - members of the public (via PDRs)

SPD and the CSCC share data collected by the NICE system according to public disclosure law or as necessary for investigations and prosecutions. Section 5 of the SIR states that SPD or the CSCC share data extracted from the NICE system servers physically located at the 9-1-1 center; those data reside in an SPD network storage managed by Seattle IT. In summary, SPD and the CSCC share data with the following entities:

- 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
- Other law enforcement agencies
- Insurance companies
- Members of the public pursuant to the Washington Public Records Act, Chapter 42.56 RCW

The SPD Crime Records Unit and the CSCC jointly manage the sharing of NICE system data with internal and external entities as outlined below:

### Data Shared by the SPD Crime Records Unit

The Crime Records Unit is responsible for responding to and fulfilling requests for 9-1-1 call audio or metadata. Requests are generally from private attorneys for litigation or requests from the public (Public Disclosure Request or PDR). Between 2021 and

2022, the Crime Records Unit fulfilled 4,514 requests. Approximately 98% of these requests were PDRs for call audio, while about 2% were legal requests for call audio.

## Data Shared by the CSCC

The CSCC responds to the following request types: discovery, law enforcement investigations, Office of Police Accountability (OPA) investigations, inter-agency, and public disclosure-legal preservation. Between 2021 and 2022, the CSCC responded to 15,056 requests. Approximately 59% of these requests originated from the Seattle City Attorney's Office, while detective requests accounted for about 33%. The remaining 8% of requests were OPA investigations, inter-agency, and legal preservation requests.

## C. Data Management and Safeguarding of Individual Information

---

9-1-1 call recording occurs whenever the CSCC answers a call. The NICE System pulls metadata from the Viper telephony system used for 9-1-1 calls and stores it along with the recording of the call. These metadata include: the address registered to the phone; the address, latitude, and longitude coordinates of the reported incident location; whether the caller is on a mobile or land line; whether the caller is using a VOIP phone system or a conventional "Plain Old Telephone Service" (POTS) line. If the caller is using a mobile device the system also automatically records the location of the nearest cellular tower to the caller. The Nice System stores these data along with the recording for up to 90 days.

### NICE System Security Review

A limited IT security review of the NICE System, including its authentication and authorization system, configuration, and backups was conducted with no concerns of note. The review was limited to the NICE System itself and did not include the underlying Windows operating system or the virtual infrastructure in which it runs, so there may be areas of IT security risk that are outside the scope of this review.

User accounts within the NICE System are configured in line with the principles of Role-Based Access Control, ensuring that each user in the system has only the level of access that is required for their job function.

Access and audit logs for the NICE System are available from the time the system was introduced in 2018. The audit logs for the NICE system show which records a user accesses, what computer was used to access them, and the date and time of

the access. This is sufficient for auditing the NICE System itself, however we note that these records only pertain to records stored in the NICE System itself and does not include evidentiary records that have been moved onto the secure shared drive.

Detailed records are kept on recordings that are placed into evidence, including the date, time and General Offense (GO) number associated the record was entered into evidence. Not all recordings have unique GO numbers. Multiple recordings may share the same General Offense number, as some types of incidents generate multiple calls to 9-1-1. We found the recordkeeping practices around reviewing and storing 9-1-1 audio recordings to be excellent and highly detailed. However, these practices are not documented as an operational procedure.

- **Recommendation 1:** CSCC should formalize current recordkeeping practices as written procedures.

## Secure Shared Network Drive

After 90 days, the NICE System automatically deletes recordings that are not retained as evidence. If CSCC staff store a recording is evidence, the callers' metadata from the Viper telephony system will be stored with it in a folder in a secure shared network drive accessible to both the NICE System administrators and SPD personnel who are using the recordings as part of their investigation. Once a recording is entered as evidence, it is retained indefinitely. Detectives must request access to the secure shared drive, and CSCC staff record each time access is given to a detective. Once access is provided, SPD detectives do not have the ability to delete or modify records stored in evidence on the shared drive. Detectives can view and download recordings from the shared drive but must use secure PDF viewer software to view metadata associated with the recorded call. The secure viewer software notes the time, date and username of the person viewing the Viper telephony system metadata in an audit log.

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

---

The 9-1-1 Logging Recorder system is designed to record individuals who are intentionally contacting police to report crimes or emergencies. Because this information may be used in a prosecution or divulged to the public as required by law, a caller may not be aware that some information divulged in a call to 911 may not be kept private or confidential.

With respect to civil liberty concerns, the Community Surveillance Working Group (CSWG) noted in a letter to SPD pertaining to the 9-1-1 Logging Recorder that a main concern was whether 9-1-1 recordings are being used as part of any data mining, machine learning or voice recognition projects. This has been noted as an area of major concern by civil rights advocates in areas where it is used in other states, who question the scientific basis of this form of analysis as well as the standards by which it is conducted.

There was no evidence that CSCC uses voice stress analysis to determine whether a caller is being dishonest when reporting a crime or emergency, nor does it factor into whether SPD responds to an incident.

## E. Complaints, Concerns and Other Assessments

---

### Office of Police Accountability (OPA) Complaints

No relevant concerns or complaints were submitted to OPA in 2021 or 2022.

### Customer Service Bureau Complaints

No relevant complaints or concerns from 2021 or 2022 were submitted to the City of Seattle Customer Service Bureau.

### Internal Audits or Assessments

No internal audits or assessments were conducted on this technology in 2021 or 2022.

## F. Cost Auditing

---

The CSCC utilizes Motorola Solution's NICE Gold-Lite package for its 9-1-1 logging recorder technology. During the 2021 calendar year, the annual renewal cost was \$49,199.18. No other costs were identified for this year.

During the 2022 calendar year, the annual renewal cost was \$51,717.91. This amount was a 5.12% increase compared to the previous year. No additional purchases or other costs were recorded.



## Surveillance Technology Usage Review

### 9-1-1 Logging Recorder (2021 and 2022)

#### *Recommendation Response*

1. CSCC should formalize current recordkeeping practices as written procedures.

#### CSCC Management Response

Concur  Do Not Concur

Estimated Date of Implementation: Q2 2024

Proposed Implementation Plan: CSCC (soon to be renamed CARE) will create written policy and procedures to formalize current recordkeeping practices as recommended.

#### **Non-Audit Statement**

This review was not conducted under Generally Accepted Government Auditing Standards (GAGAS); however, OIG has followed GAGAS standards regarding the sufficiency and appropriateness of evidence.