

2026 Surveillance Impact Report Executive Summary

Emergency Response Aerial Technology

Seattle Fire Department

Overview

The purpose of this Executive Summary is to highlight policies, technology and practices regarding the surveillance technologies under Council review. This document outlines information, including policies and practices, about the collection, use, sharing, security and access controls for data that is gathered using a technology or program. All information provided here is contained in the body of the full SIR document but is provided in a condensed format for easier access and consideration.

1.0 Purpose

The mission of the Seattle Fire Department is to save lives and protect property through emergency medical service, fire and rescue response, and fire prevention. We respond immediately when any member of our community needs help with professional, effective, and compassionate service. SFD is proposing to add three emergency response aerial technology (ERAT) devices, also commonly called drones, to the list of specialty equipment we use on specific emergency calls. The ERAT will only be used for a small and defined set of incident types to provide additional visual situational awareness and firefighter safety, particularly in situations where firefighters at ground level are unable to see the full scope of the emergency. When dispatched, the ERAT will fly to a specific latitude and longitude with camera aimed at the horizon. After arriving, the camera will be pointed downward at the scene to provide a live feed for trained Seattle Fire incident commanders and dispatchers, to view and help make operational decisions. The feed will not be recorded or saved in any way. No one besides SFD responders may watch the drone livestream. SFD will not use the drone feed for any enforcement purposes.

The purpose of the Seattle Fire Department ERAT program is to enhance SFD's lifesaving emergency response capabilities when we respond to any member of the public who needs our help, and to improve firefighter safety.

2.0 Data Collection and Use

Video (to include audio and thermal imaging) will not be stored. The live feed is streamed to the operator and a small number of approved on-duty Chiefs who are part of the response. This data will be used to enhance SFD's emergency response services and support firefighter safety. SFD personnel will be trained and responsible for complying with privacy and security requirements from the City of Seattle and SFD.

The following data will be stored and have [State of Washington retention/destruction periods](#) applied:

- List of pilot names, associated emails and the live ops team they are on, SFD employee user's phone numbers, user management logs.
- List of ERAT device names.
- Aggregate and by-device data on the count of flights, hours online, distance travelled.
- Pre- and post-flight inspections records.
- Data published to SFD's public transparency dashboard.

- Data supporting reports to the Federal Aviation Administration (FAA) regarding air space incursions, etc.
- List of SFD users who are set up to receive secure email links to the ERAT feed.
- Audit log of users who look at, modify or delete any Seattle data in the software system.
- Station launch locations and ERAT locations.
- Major and regulated maintenance history, minor non-regulated maintenance history, and ERAT conditions such as any trouble or maintenance indicators.
- Tech support tickets (to include returned merchandise authorization for ERAT or related equipment).

Flights logs are required to be maintained by the FAA and include flight dates, times, and durations; the aircraft registration number; the purpose of the operation; the flight path including destination, origin, and altitudes; the name of the designated operations personnel assigned to each flight; and landing locations.

3.0 Data Minimization & Limitations

ERATs will be launched only by a small number of specially trained SFD members who are detailed to the role of Firefighter/Dispatcher at the SFD Fire Alarm Center. Use of ERAT will be limited and controlled. SFD Firefighter/Dispatchers will verify that the incident type is appropriate for the use of ERAT (consistent with this SIR) prior to dispatching the ERAT. An FAA operational safety checklist must also be performed each day and as part of each flight.

ERAT shall travel to incidents with an “eyes up” approach until at the defined incident location, when cameras will be pointed down.

Video including audio and thermal imaging will not be recorded.

Records shall be maintained of all flight operators as well as all personnel who are authorized to receive, and who has received, encrypted video links of the live stream. Records are also maintained of all individuals who create, modify, or delete data in the ERAT vendor’s software system.

4.0 Access & Security

Access

Before having access to pilot ERAT or to receive ERAT live video feeds, SFD personnel will receive specific privacy training related to compliance with Chapter 14 of the Seattle Municipal Code. All SFD employees will also receive annual privacy awareness training. The training will be recorded and tracked in the SFD learning management system.

Live video feeds will be sent by encrypted link to authorized users only. Two-factor authentication will be used for authorized users. Video stream access links are incident- and employee-specific, and shall expire once the incident is closed.

The live video may not be shared outside of SFD. Sharing is prohibited with employees from other City departments, or other state, local or federal agencies or governments, or other

organizations or bystanders. The contract with the vendor will limit vendor access to Seattle data to technical troubleshooting purposes only.

SFD has drafted strict operating guidelines to prevent non-authorized access to live video streams.

SFD supervisors and commanding officers are responsible for ensuring compliance with use and management policies. The SFD FAC Fire Alarm Center Captain will be responsible for ensuring compliance with FAA requirements. SFD's Public Disclosure Officer can also conduct audits of all data collection software and systems. Additionally, any appropriate auditor, including the City Auditor's Office, can audit at any time.

Security

Data will be protected by the following security standards:

- Federal information processing standard 140-2 is met for all data and data is encrypted based on the AES-256 standard.
- Data is stored on a US based AWS server and data is only accessible to authorized to specific SFD employees in specific roles on duty, under its secured organization accounts.
- CJIS-compliant system, meaning the system adheres to the FBI's strict criminal justice information security policy. This includes user access tracking, ensuring there is an access log of any access to any potentially sensitive information.
- The cloud-based system is also SOC2 compliant, a standard set by the AICPA (American Institute of Certified Public Accountants). SOC2 certified that a service organization securely manages data to protect privacy and system reliability.
- In terms of audit trails and information about access, several mechanisms will be available to SFD. A flight log is maintained that lists SFD operators. A list is maintained of employees who are approved to receive encrypted live video feed and their email addresses – on-duty Chiefs involved in the incident response. A list is maintained of the email addresses of individuals to whom the encrypted link to the ERAT live feed is sent. These lists can be queried and audited at any time.
- The vendor also provides audit logs related to data access, data modification and/or deletion. It is possible to query this information and learn who accessed, modified or deleted Seattle data at any time.

5.0 Data Sharing and Accuracy

No data sharing with any partners are proposed, this data is only for limited, focused SFD emergency use. Live video streams will not be recorded or shared.

The ERAT contractor will have strict contractual terms limiting access to Seattle data for technical troubleshooting purposes.

6.0 Data Retention

Unit supervisors are responsible for ensuring compliance with data retention requirements in SFD. The SFD Fire Alarm Center Captain will be responsible for maintaining the flight logs and other data that must be retained per [laws of Washington State](#). The vendor's system will be programmed to delete data once the State record's retention period has been reached, consistent with State retention and destruction guidelines. SFD's Public Disclosure Unit personnel can also conduct audits of all data collection software and systems to ensure vendor compliance with retention laws and periods that will be incorporated into SFD's contract with the vendor. Additionally, any appropriate auditor, including the City of Seattle Auditor's Office, can audit for compliance at any time.