



2025 Privacy Impact Assessment

FlashCAM: SPR Theft and Vandalism Cameras

Seattle Parks and Recreation FAST Division



Seattle
Information Technology
03/14/2025

Privacy Impact Assessment overview	2
What is a Privacy Impact Assessment?	2
When is a PIA required?	2
How to complete this document?	2
1.0 Abstract	3
2.0 Project / Technology Overview	3
3.0 Use Governance	6
4.0 Data Collection and Use	7
5.0 Data Storage, Retention and Deletion	12
6.0 Data Sharing and Accuracy	15
7.0 Legal Obligations, Risks and Compliance	18
8.0 Monitoring and Enforcement	21

Privacy Impact Assessment overview

What is a Privacy Impact Assessment?

A Privacy Impact Assessment (“PIA”) is a method for collecting and documenting detailed information collected in order to conduct an in-depth privacy review of a program or project. It asks questions about the collection, use, sharing, security, and access controls for data that is gathered using a technology or program. It also requests information about policies, training and documentation that govern use of the technology. The PIA responses are used to determine privacy risks associated with a project and mitigations that may reduce some or all of those risks. In the interests of transparency about data collection and management, the City of Seattle has committed to publishing all PIAs on an outward facing website for public access.

When is a PIA required?

A PIA may be required in two circumstances.

- When a project, technology, or other review has been flagged as having a high privacy risk.
- When a technology is required to complete the Surveillance Impact Report process. This is one deliverable that comprises the report.

How to complete this document?

As department staff complete the document, they should keep the following in mind.

- Responses to questions should be in the text or check boxes only, all other information (questions, descriptions, etc.) should **NOT** be edited by the department staff completing this document.
- All content in this report will be available externally to the public. With this in mind, avoid using acronyms, slang, or other terms which may not be well-known to external audiences. Additionally, responses should be written using principally non-technical language to ensure they are accessible to audiences unfamiliar with the topic.

1.0 Abstract

1.1 Please provide a brief description (one paragraph) of the purpose and proposed use of the project/technology.

Vandalism, theft, graffiti, and illegal dumping have become growing concerns at Seattle Parks and Recreation (SPR) facilities and sites. To support investigations of these incidents, SPR proposes the deployment of a camera system on park properties. These cameras will capture images for later review, and if a post-incident assessment determines reasonable suspicion of criminal activity, the relevant photos may be securely submitted to the appropriate law enforcement agency.

1.2 Explain the reason the project/technology is being created or updated and why the PIA is required.

In recent years, Seattle Parks and Recreation (SPR) has responded to a significant increase in vandalism, theft, graffiti, and illegal dumping across the city. Offenders frequently target parks and recreational facilities during late hours or in remote locations, leading to the loss of City assets, damage to public property, safety hazards, and substantial maintenance and replacement costs. To enhance security monitoring and deter criminal activity in high-risk areas, SPR will implement FlashCAM technology as a proactive security measure.

2.0 Project / Technology Overview

Provide an overview of the project or technology. The overview gives the context and background necessary to understand the purpose, mission and justification for the project / technology proposed

2.1 Describe the benefits of the project/technology.

The implementation of this technology empowers Seattle Parks and Recreation (SPR) to detect and identify potential violators, enhancing its ability to respond to incidents while deterring future offenses. Beyond capturing evidence, the system acts as a proactive deterrent, utilizing motion-triggered alerts such as strobe flashes and audible warnings to prevent theft and vandalism before they occur. By deploying this technology in high-risk areas, SPR aims to reduce criminal activity, safeguard public assets, and uphold the safety and integrity of park facilities.

2.2 Provide any data or research demonstrating anticipated benefits.

Other City departments, such as Seattle Public Utilities (SPU) Clean City team, have chosen the Q-Star FlashCAM due to its advanced voice warning system. This system provides a verbal alert to potential illegal dumpers, offering them the opportunity to leave the area before any photos are taken. The goal is to deter individuals from committing violations by encouraging them to vacate the premises, thereby reducing the need for enforcement actions and minimizing the submission of photographic evidence to law enforcement.

Several municipalities across the country have successfully implemented similar camera systems to combat illegal dumping and vandalism, including:

- **City of Palm Desert, CA**
[Link to policy document](#)
- **City of Inglewood, CA**
[Link to policy document](#)
- **El Paso, TX**
[Link to article on safety and security solutions](#)

By leveraging the proven effectiveness of FlashCAM technology and learning from other municipalities, Seattle Parks and Recreation aims to enhance security, reduce crime, and protect public spaces.

2.3 Describe the technology involved.

Q-Star FlashCAM is an advanced security solution designed to assist cities and counties in safeguarding public spaces from theft, vandalism, illegal dumping, and graffiti. This state-of-the-art camera system offers a proactive approach to crime prevention by integrating a **motion-activated strobe flash** and a **customizable voice warning**, which serve to deter potential offenders before illegal activity occurs.

The FlashCAM system captures photos of unauthorized activity. These images can be reviewed by **Seattle Parks and Recreation (SPR) personnel** to assess incidents and, if necessary, coordinate with law enforcement for further investigation.

To ensure privacy and data security, access to any footage or information collected by the FlashCAM system will be strictly limited to **authorized SPR personnel**. This controlled access helps maintain confidentiality while supporting SPR's mission to protect public assets, enhance security, and promote safer community spaces.

2.4 Describe how the project or use of technology relates to the department's mission.

Cameras will be deployed on **City-owned buildings and sites** that have been repeatedly targeted for **theft, vandalism, graffiti, and illegal dumping**, particularly in locations where such activities hinder **public access and enjoyment**. These cameras will be **motion-activated**, capturing images when an individual or vehicle enters the monitored area, allowing for documentation of illegal activities.

This initiative directly supports **Seattle Parks and Recreation's (SPR) mission** to maintain open and accessible public spaces, **prevent site closures**, and preserve the **beauty and integrity** of parks and facilities for all visitors. By proactively deterring criminal behavior, the technology helps ensure that community members can continue to enjoy clean, safe, and well-maintained public areas.

Additionally, the use of this technology enhances the **efficiency of incident response** by enabling faster **collection, review, and analysis of evidence** by subject matter experts. This streamlined process allows for **quicker decision-making** and, when necessary, expedites communication with **law enforcement** to support investigations and enforcement actions.

2.5 Who will be involved with the deployment and use of the project / technology?

Seattle Parks and Recreation's (SPR) **Facilities, Access, Automation, Security Systems, and Technology (FAST) unit** is responsible for overseeing the deployment, operation, and maintenance of this security technology. As part of its commitment to enhancing safety and protecting public assets, **SPR will strategically install cameras** on designated **City-owned buildings, infrastructure, and poles** in areas identified as high-risk for theft, vandalism, graffiti, and illegal dumping. These installations will be carefully planned to ensure optimal coverage while adhering to **privacy and legal guidelines**, reinforcing SPR's mission to maintain secure and accessible public spaces.

3.0 Use Governance

Provide an outline of any rules that will govern the use of the project / technology. Please note non-City entities are bound by restrictions specified in the Surveillance Ordinance and Privacy Principles and must provide written procedures for how the entity will comply with any restrictions identified.

3.1 Describe the processes that are required prior to each use, or access to/ of the project / technology, such as a notification, or check-in, check-out of equipment.

Security Monitoring & FlashCAM Deployment

Identification of High-Risk Locations

Buildings and locations with repeated incidents of theft, vandalism, graffiti, and illegal dumping will be identified through data collected from SPR's Asset Management Work Order System (AMWO) and reports from SPR staff, management, and the executive team. Additionally, the surrounding environment, including residential, commercial, park, and mixed-use areas, will be considered.

Security Signage

Clear signage will be posted to indicate: "**Security cameras are in operation 24/7.**"

FlashCAM Deployment & Functionality

FlashCAM cameras will be strategically positioned to monitor only City-owned property and facilities. Each camera is capable of storing between **1,800 and 3,000 images**. When storage reaches capacity, the system is configured to automatically overwrite the oldest images in a **First-In, First-Out (FIFO)** manner.

Access & Data Security

- Only the FAST unit has access to retrieve images from the cameras.
- Camera footage is protected by secure passwords, accessible only by designated System Administrators.
- The cameras will activate **only when a person or vehicle enters restricted areas outside operational hours**.

Deterrence Features

Before capturing images, the camera system provides a **motion-triggered warning**, including:

- A **strobe flash** to alert potential intruders.
- A **customizable voice warning** to deter unauthorized activity.

Image Management & Privacy Protection

- No prior check-out is required for use—only a login to access camera memory.
- SPR FAST unit personnel will conduct regular camera inspections.
- Any unrelated images of individuals, vehicles, or activities **not linked to illegal activity** will be **permanently deleted**.
- Any individuals or vehicles **not involved in criminal acts** will be **masked, covered, or cropped out** to ensure privacy.
- Only images related to confirmed illegal activity will be securely stored in the Department's file system, accessible exclusively to the SPR FAST team.

3.2 List the legal standards or conditions, if any, that must be met before the project / technology is used.

Seattle Parks and Recreation (SPR) is **not designated as an enforcement agency** for **theft, vandalism, graffiti, or illegal dumping** incidents within the corporate limits of the **City of Seattle**. While SPR plays a critical role in **monitoring and protecting public spaces**, the enforcement and prosecution of such crimes remain under the jurisdiction of **local law enforcement agencies**.

To ensure the responsible use of this technology, **all personnel within the Facilities, Access, Automation, Security Systems, and Technology (FAST) unit** are required to complete and maintain **good standing in Privacy and Information Security Awareness Training**. This training ensures that staff adhere to **strict data protection protocols** and uphold the highest standards of **confidentiality and ethical use** of collected information.

Any **footage or images** captured by the **FlashCAM system** that include individuals or vehicles will be handled with **utmost security and confidentiality**. If deemed necessary for an investigation, relevant footage will be securely transferred to **law enforcement authorities**, ensuring compliance with **privacy laws and departmental policies** while supporting efforts to address criminal activity in Seattle's public spaces.

3.3 Describe the policies and training required of all personnel operating the project / technology, and who has access to ensure compliance with use and management policies.**Policies, Training, and Access Controls for Technology Operation**

All personnel operating the **FlashCAM system** under **Seattle Parks and Recreation (SPR)** are required to adhere to strict policies and undergo specialized training to ensure the **ethical, secure, and compliant** use of this technology.

Training Requirements:

Personnel within SPR's **Facilities, Access, Automation, Security Systems, and Technology (FAST) unit** must successfully complete **Privacy and Information Security Awareness Training** and remain in **good standing** throughout their tenure. This training ensures that staff:

- Understand **privacy laws, data security protocols, and ethical considerations** related to personal information.
- Follow **proper procedures** for handling, storing, and reviewing captured footage.
- Maintain **confidentiality and security** when managing images and data.

Access Controls & Compliance:

To safeguard **sensitive information**, access to the **FlashCAM system and its data** is strictly **limited to authorized FAST unit personnel**. This ensures:

- **Secure storage and restricted access** to recorded footage.
- That only **relevant and necessary images** related to suspected criminal activity are **reviewed and, if warranted, shared with law enforcement**.
- That **unrelated or incidental footage** (e.g., images of bystanders or non-relevant vehicles) is permanently **deleted or redacted** to maintain privacy standards.

These policies and training requirements ensure that the **use and management** of the FlashCAM system comply with **legal, ethical, and departmental standards**, reinforcing SPR's commitment to **protecting public spaces while upholding individual privacy rights**.

4.0 Data Collection and Use

Provide information about the policies and practices around the collection and use of the data collected.

4.1 Provide details about what information is being collected from sources other than an individual, including other IT systems, systems of record, commercial data aggregators, publicly available data and/or other city departments.

Seattle Parks and Recreation's (SPR) **Facilities, Access, Automation, Security Systems, and Technology (FAST) unit** will be solely responsible for the **collection, management, and oversight** of all data generated by the **FlashCAM system**. To ensure **security, integrity, and confidentiality**, all captured images and associated data will be **handled exclusively by authorized FAST personnel** and will not be shared with any **third-party vendors** for review or processing.

This technology is designed with **strict privacy safeguards**, and it does **not collect, integrate, or analyze** data from any **external sources** beyond its intended purpose of monitoring and documenting incidents of **theft, vandalism, graffiti, and illegal dumping** on City-owned properties.

All recorded information will be securely stored on a **designated City of Seattle server**, which is protected by **robust cybersecurity measures** to prevent unauthorized access, modification, or distribution. This approach ensures that **all data remains under the direct control of the City** while complying with **privacy regulations, security protocols, and ethical standards** governing surveillance operations.

4.2 What measures are in place to minimize inadvertent or improper collection of data?

Seattle Parks and Recreation (SPR) is actively developing a comprehensive policy for the **Facilities, Access, Automation, Security Systems, and Technology (FAST) unit** to govern the **responsible and acceptable use** of the FlashCAM system. This policy will align with **current and future Seattle Municipal Code (SMC), ordinances, and evolving data privacy regulations** to ensure compliance with legal and ethical standards. Additionally, the policy will establish **clear guidelines** for the **storage, management, and controlled sharing of captured images with law enforcement agencies** when necessary.

Strict Privacy Measures

SPR is committed to protecting the privacy of individuals. As part of this policy:

- Any **photos capturing individuals not involved** in theft, vandalism, graffiti, or illegal dumping on SPR property will be **permanently deleted**.
- If a **photo does not contain evidence** of illegal activity, it will be **immediately discarded** upon review.
- In instances where persons or vehicles appear in images but **are not connected** to illegal activities, they will be **redacted, covered, or cropped out** to prevent unauthorized identification or exposure.

Camera Placement and Activation

FlashCAM units will be **strategically placed** to monitor and capture images **exclusively within City-owned parks and facilities**, ensuring that only **public property with limited public access** is recorded. Measures will be taken to **mask or obscure private properties** adjacent to monitored locations, reinforcing SPR's commitment to **targeted enforcement without infringing on individual privacy rights**.

The FlashCAM system is **motion-activated**, meaning:

- Once movement is detected, there is a **30-second delay** before the camera initiates a **bright flash** to illuminate the area.
- A **pre-recorded voice message** will then play, warning individuals that the area is being monitored and instructing them to leave.
- The warning explicitly states that if they **choose to remain**, their actions **will be recorded** for further review.

Public Notification & Transparency

To maintain **public awareness and transparency**, SPR will install **clear, visible signage** at monitored locations, informing visitors that **security cameras are in operation**. These notices will help **deter unlawful behavior** while ensuring that the public is fully informed of **camera usage** to protect City assets and public spaces.

4.3 How and when will the project / technology be deployed or used? By whom? Who will determine when the project / technology is deployed and used?

Seattle Parks and Recreation (SPR) is launching a **pilot program** to deploy FlashCAM systems at **select high-risk locations** within its parks and recreational facilities. The **Facilities, Access, Automation, Security Systems, and Technology (FAST) unit** will oversee the **planning, installation, and ongoing management** of the technology. The program is scheduled to launch in **March or April of 2025** and will be continuously monitored for effectiveness.

The **decision to deploy and operate the FlashCAM system** will be made by SPR's **FAST unit**, in coordination with **department leadership and other relevant city officials**. Deployment locations will be determined based on **data-driven analysis of prior incidents of theft, vandalism, graffiti, and dumping**.

To ensure a **secure and effective installation**, the deployment process may involve collaboration with SPR's **electrical, carpentry, and metal fabrication units**, who will assist with the **mounting, wiring, and structural support** of the FlashCAM system. These cameras

will be **strategically placed on SPR-owned poles and buildings** to maximize coverage while adhering to **privacy and security protocols**.

Once deployed, the FlashCAM system will operate **continuously**, with **motion-activated features** designed to capture and document illegal activities. The **FAST unit will oversee the daily use of the technology**, ensuring compliance with operational guidelines, privacy policies, and law enforcement collaboration when necessary.

The **pilot phase** will allow SPR to **assess the effectiveness** of the FlashCAM system, refine **deployment strategies**, and ensure alignment with **best practices for crime deterrence and documentation**.

4.4 How often will the technology be in operation?

The FlashCAM system will be operational in designated areas **seven days a week, up to 24 hours a day**, providing continuous security monitoring of SPR-owned spaces to deter and document unauthorized activities. The system is **motion-activated**, meaning it only engages when movement is detected within its monitoring range.

Upon activation, the FlashCAM will initiate a **30-second delay** before capturing any images. During this time, a **high-intensity strobe flash** will illuminate the area, and a **prerecorded voice message** will audibly warn individuals that security cameras are in use in the area. The warning will instruct individuals to **leave the premises immediately** to avoid being photographed. If the individual(s) vacate the area within the warning period, no photos will be taken. However, if the unauthorized presence continues, the FlashCAM will proceed to capture images for potential review.

The **Facilities, Access, Automation, Security Systems, and Technology (FAST) unit** will regularly evaluate the effectiveness of the cameras. If illegal activities in monitored areas significantly **decrease**, the FAST team will assess whether the cameras should be **relocated** to other high-risk areas experiencing increased incidents of theft, vandalism, graffiti, or dumping within SPR properties and sites. This strategic approach ensures that the FlashCAM system is deployed where it is most needed to support public safety, asset protection, and the continued enjoyment of Seattle Parks and Recreation facilities.

4.5 What is the permanence of the installation? Is it installed permanently or temporarily?

The FlashCAM system will be deployed either **temporarily or repositioned** based on ongoing assessments of security needs. Its placement will be determined by the prevalence of illegal activities such as theft, vandalism, graffiti, and dumping within Seattle Parks and Recreation (SPR) properties.

When monitoring data indicates a **decline in illegal activity** at a specific location, the **Facilities, Access, Automation, Security Systems, and Technology (FAST) unit** will evaluate whether the camera should remain in place or be **relocated to a different high-risk area**. This dynamic approach ensures that the FlashCAM system is continuously utilized in locations where it can provide the greatest benefit in **enhancing public safety, protecting park assets, and maintaining the cleanliness and accessibility of recreational spaces**.

4.6 Is a physical object collecting data or images, visible to the public? What are the markings to indicate that it is in use? What signage is used to determine department ownership and contact information?

The camera monitor will be installed on a City-owned poles, structure, or buildings and may potentially be viewed by onlookers or the public.

Signage will also be placed in a visible area notifying the public in the area the FlashCAM is in use.

4.7 How will data that is collected be accessed and by whom?

Data collection occurs **only when the cameras are activated by motion**, ensuring that images are captured solely in response to detected activity. All photographs taken by the FlashCAM system will be **reviewed exclusively by authorized Seattle Parks and Recreation (SPR) personnel** and will remain **accessible only to the Facilities, Access, Automation, Security Systems, and Technology (FAST) unit**.

In certain instances, **if an image provides evidence of a violation**, such as theft, vandalism, graffiti, or illegal dumping it may be **shared with the appropriate law enforcement agencies** to support the enforcement of fines or other legal actions as required.

To maintain **data security and confidentiality**, all images will be **transferred from the camera to a secure laptop** before being permanently **stored on a secure City of Seattle drive or server**. If a review determines that **no illegal activity was captured**, the photograph will be **immediately deleted** to protect individual privacy and ensure compliance with data management policies.

4.8 If operated or used by another entity on behalf of the City, provide details about access, and applicable protocols. Please link memorandums of agreement, contracts, etc. that are applicable.

No external entity will have access to or operate the FlashCAM system on behalf of Seattle Parks and Recreation (SPR). **All data collected by the cameras will be strictly managed and accessed exclusively by authorized SPR personnel within the Facilities, Access, Automation, Security Systems, and Technology (FAST) unit.**

No third-party vendors, contractors, or external agencies will have direct control over or permission to view, store, or process the images captured by the FlashCAM system. **Access to the data is restricted** to ensure compliance with security protocols, protect individual privacy, and uphold SPR's data management policies.

If any images provide evidence of illegal activity, they may be **shared with appropriate law enforcement agencies** for investigative or enforcement purposes. However, this will be done **in accordance with established policies and procedures**, ensuring that only relevant images related to confirmed violations are disclosed.

At this time, **no memorandums of agreement, contracts, or other legal agreements** exist regarding the operation or management of FlashCAM data by external entities. Should any future agreements be developed, they will be documented and made available as appropriate.

4.9 What are acceptable reasons for access to the equipment and/or data collected?

Acceptable Reasons for Access to FlashCAM Equipment and Data

Access to the FlashCAM system and any data it collects is strictly controlled and limited to authorized personnel within Seattle Parks and Recreation's (SPR) **Facilities, Access, Automation, Security Systems, and Technology (FAST) unit**. The following are considered **acceptable reasons** for accessing the equipment and/or reviewing collected data:

- **Investigation of Theft, Vandalism, Graffiti, and Illegal Dumping:** Data may be accessed to identify and document incidents of property damage, unauthorized activity, or unlawful disposal of waste on SPR properties. This information may be used to support enforcement actions or preventative measures.
- **Public Records Requests:** In accordance with applicable laws, certain data may be subject to public records disclosure. However, **exemptions may apply** to protect personal privacy, ongoing investigations, or other legally sensitive information.
- **Litigation Discovery:** Data may be accessed and reviewed as part of legal proceedings, in compliance with discovery requirements, court orders, or other legal obligations.
- **Collaboration with Law Enforcement Agencies:** When necessary, images or other data may be **shared with law enforcement agencies** to aid in criminal investigations, issue citations, or support prosecution related to unlawful activities occurring on SPR property.

Security and Compliance Measures

Access to FlashCAM data is **limited to authorized personnel** and will be managed in accordance with SPR's data security policies. Any data that does not pertain to illegal activity will be promptly deleted, and images containing individuals or vehicles **not involved in a violation will be redacted, masked, or cropped** to protect privacy.

These policies ensure that the use of the FlashCAM system remains **focused on its intended purpose of deterring and documenting criminal activity** while upholding **data security, privacy, and legal compliance standards**.

4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) and to provide an audit trail (viewer logging, modification logging, etc.)?

Safeguards for Protecting Data and Maintaining an Audit Trail

To ensure the security and integrity of data collected by the FlashCAM system, Seattle Parks and Recreation (SPR) has implemented **robust safeguards** to prevent unauthorized access and maintain a comprehensive audit trail.

Data Security Measures

- **Secure Storage:** Photos and related data capturing illegal activities will be stored exclusively on a **secured City of Seattle server or drive**, accessible **only** to authorized members of the **Facilities, Access, Automation, Security Systems, and Technology (FAST) unit**.

- **Access Controls:** Strict **role-based access control (RBAC)** mechanisms will be in place to limit access to personnel with specific authorization. Unauthorized users will not be able to access or modify the data.
- **Encryption:** Data will be encrypted **both in transit and at rest** to prevent unauthorized interception or tampering.
- **Secure Transfer Protocols:** Photos will be securely transferred from the FlashCAM system to a **designated, encrypted laptop** before being stored on a secure server or drive.

Audit and Compliance Measures

- **Access Logging:** All interactions with the stored data, including viewing, downloading, or sharing, will be logged to maintain a **detailed audit trail**.
- **Modification Tracking:** Any edits, redactions, or deletions of data will be **logged and reviewed** to ensure compliance with SPR policies and legal requirements.
- **Policy Development:** A **new policy** will be established to standardize the tracking, retention, and logging of data related to potential **theft, vandalism, graffiti, and illegal dumping** incidents.
- **Retention and Deletion:** Any data that does not pertain to an illegal act will be **immediately deleted**. Data related to verified incidents will be retained in accordance with legal and policy guidelines.

These safeguards ensure that the FlashCAM system operates **in compliance with data security best practices, protects privacy**, and maintains **transparency and accountability** in its usage.

5.0 Data Storage, Retention and Deletion

5.1 How will data be securely stored?

Secure Storage of FlashCAM Data

To ensure the **security, integrity, and confidentiality** of data collected by the FlashCAM system, Seattle Parks and Recreation (SPR) has implemented **strict access controls and secure storage protocols**.

Access Control & Data Protection

- **Restricted Access:** Only **authorized members** of the **Facilities, Access, Automation, Security Systems, and Technology (FAST) unit** have access to the secured server or drive where the data is stored.
- **Executive & HR Viewing Protocol:** While the **Executive Team** and **Human Resources (HR)** may review footage when necessary, their access will be **strictly limited** to a **secured, non-downloadable link**, preventing any unauthorized copying or distribution.
- **Secure Data Transfer:**
 - Photos captured by the FlashCAM system will **remain stored on the camera** until securely transferred.

- Data will be **downloaded to a secured laptop** before being permanently stored on a **secured City of Seattle server or drive** with **encryption and access controls** in place.
- **Automatic Overwrite Mechanism:** The camera can store between **1,800 to 3,000 images**. Once the memory reaches capacity, the system can be configured to **automatically overwrite the oldest images** using a **First In, First Out (FIFO)** approach, ensuring efficient storage management.

Regular Inspections & Data Deletion

- **Camera Inspections:** The FAST team will conduct **regular inspections** of the FlashCAM system to verify its functionality and ensure compliance with **data retention policies**.
- **Unrelated Data Deletion:** During these inspections, any **unrelated photos**—including those capturing **individuals, vehicles, or activities unrelated to theft, vandalism, graffiti, or illegal dumping**—will be **permanently deleted** from the camera's memory.
- **Retention Policy:** Only **photos directly related to illegal activities** will be stored on the **Department's secured server or drive**, accessible **exclusively by the FAST unit** in accordance with **data security and privacy regulations**.

These measures ensure **responsible data management, prevent unauthorized access, and maintain public trust in SPR's efforts to enhance security** across its properties.

5.2 How will the owner allow for departmental and other entities, to audit for compliance with legal deletion requirements?

The **Facilities, Access, Automation, Security Systems, and Technology (FAST) unit** within **Seattle Parks and Recreation (SPR)** is responsible for ensuring that all **data management, retention, and deletion policies** comply with **legal requirements and departmental guidelines**.

Compliance Oversight & Auditing

To ensure transparency and adherence to **legal deletion requirements**, the following safeguards and auditing measures will be in place:

- **Regular Internal Audits:** The FAST unit will conduct **scheduled audits** of stored data to verify that any **unrelated images** (e.g., individuals, vehicles, or activities not related to illegal dumping, theft, vandalism, or graffiti) are **permanently deleted** in accordance with established policies.
- **Departmental Oversight:** SPR's **executive leadership** and **legal team** will have the ability to review audit reports to ensure that all deletion policies are being followed and that only **relevant data** is retained.
- **Interdepartmental Audits:** Other City of Seattle departments with relevant oversight authority may **request an audit** to confirm compliance with **privacy regulations, public records laws, and municipal codes**.

- **Automated Deletion Protocols:** Any **photographs not containing evidence of illegal activity** will be **immediately deleted** from the system, and only images related to confirmed violations will be stored on SPR's **secured server or drive**.

Transparency & Compliance Reporting

- **Documentation & Tracking:** The FAST unit will maintain **detailed records** of all data deletions and modifications, ensuring a **clear audit trail** for compliance review.
- **Public Records Requests:** If applicable, data will be reviewed under **public records laws**, with exemptions applied as necessary to protect **privacy and sensitive information**.
- **Law Enforcement & Legal Compliance:** In cases where images are shared with law enforcement for investigations, proper documentation will be maintained to ensure **lawful data handling** and deletion once the case is resolved.

By implementing these **robust auditing and compliance measures**, SPR ensures that all data deletion practices align with **privacy laws, legal requirements, and public trust expectations** while maintaining the integrity of its security initiatives.

5.3 What measures will be used to destroy improperly collected data?

Seattle Parks and Recreation (SPR) is committed to **protecting privacy and ensuring compliance** with data retention policies. To that end, the **Facilities, Access, Automation, Security Systems, and Technology (FAST) unit** follows strict protocols for identifying and permanently deleting **improperly collected data** from the FlashCAM system.

Deletion Protocols & Review Process

- **Immediate Review & Deletion:** Any **photos not related to theft, vandalism, graffiti, illegal dumping, or other criminal activity** will be **immediately deleted** upon review by the FAST team.
- **Redaction & Data Masking:** If a photo contains **unrelated individuals or vehicles**, but still serves as evidence of a violation, SPR personnel will **redact, crop, or cover** any **non-relevant details** before storing or sharing the image.
- **Device-Level Deletion:** Improperly collected data will be **deleted directly from the FlashCAM device** during routine camera inspections, ensuring that irrelevant images do not remain stored in the system.
- **Secure Data Disposal:** Deleted images will not be **recoverable** after removal from the device or secured server. The system's **First In, First Out (FIFO) overwrite setting** will further prevent long-term storage of unnecessary data.
- **Retention Compliance:** All deletions will be conducted **in accordance with SPR's official data retention schedule**, ensuring alignment with departmental policies and legal requirements.

By implementing these **strict data destruction measures**, SPR ensures that **only relevant and necessary information is retained**, protecting the privacy of the public while effectively deterring illegal activities.

5.4 Which specific departmental unit or individual is responsible for ensuring compliance with data retention requirements?

The **Facilities, Access, Automation, Security Systems, and Technology (FAST) unit** within the **Facilities Division of Seattle Parks and Recreation (SPR)** is responsible for ensuring compliance with all **data retention policies and procedures** related to the FlashCAM system.

The **FAST unit's manager** holds ultimate responsibility for ensuring that all data collection, storage, and deletion processes **adhere to SPR's retention schedule, privacy policies, and applicable legal requirements**. This includes:

- **Overseeing data management** to ensure that photos and related information are properly stored, reviewed, and deleted in accordance with department policies.
- **Ensuring compliance with legal retention requirements**, including timely removal of data that is no longer necessary.
- **Conducting audits and assessments** to verify that data retention and deletion practices are being followed correctly.
- **Providing training and guidance** to FAST team members to uphold security and privacy protocols.

Through these oversight measures, the FAST unit ensures that all data retention requirements are **met, monitored, and enforced**, maintaining accountability and compliance with SPR policies.

6.0 Data Sharing and Accuracy

6.1 Which entity or entities inside and external to the City will be data sharing partners?

Seattle Parks and Recreation (SPR) may share data captured by the **FlashCAM system** with specific entities inside and external to the City in cases where **theft, vandalism, graffiti, illegal dumping, or other criminal activity** has been documented.

- **Internal Data Sharing:** If an incident is recorded, the data may be shared with the **City's Law Department** for legal review and to determine appropriate enforcement actions.
- **External Data Sharing:** When necessary, captured images may also be provided to **law enforcement agencies** for investigation and potential prosecution of criminal activities.

To ensure **transparency and accountability**, SPR is actively working to **develop a formal policy update** that will define the **specific procedures and limitations** regarding how data from this technology is shared. This policy will align with **privacy regulations, legal requirements, and departmental protocols** to ensure responsible handling of all collected data.

6.2 Why is data sharing necessary?

Data sharing is essential to **support public safety, protect public assets, and ensure accountability** for unlawful activities occurring on Seattle Parks and Recreation (SPR) properties. Camera footage captured by the **FlashCAM system** may provide **critical evidence** of criminal behavior, allowing for appropriate enforcement actions to be taken.

In addition to **theft, vandalism, graffiti, and illegal dumping**, SPR personnel may identify other forms of unlawful activity through camera footage, such as **drug-related offenses or firearm use** on park properties. When such incidents are documented, they will be reported to the **City's Law Department for legal review** and, if necessary, shared with **law enforcement agencies** to assist in investigations and enforcement efforts.

By sharing relevant data with law enforcement partners, SPR aims to **enhance security, deter future criminal activity, and maintain safe and accessible public spaces for all community members**.

6.3 Are there any restrictions on non-City data use?

Yes ☐ No ☒

6.3.1 If you answered Yes, provide a copy of the department's procedures and policies for ensuring compliance with these restrictions.

N/A

6.4 How does the project/technology review and approve information sharing agreements, memorandums of understanding, new uses of the information, new access to the system by organizations within City of Seattle and outside agencies?

Seattle Parks and Recreation (SPR) is committed to **responsible data management and information sharing** in compliance with legal and privacy standards. The department will develop a **comprehensive policy** outlining the **acceptable use, data retention, and information-sharing protocols** related to the FlashCAM system. This policy will specifically address the handling of data collected in cases of **theft, vandalism, graffiti, illegal dumping, and other criminal activities** occurring on SPR property.

Any new **information-sharing agreements, memorandums of understanding (MOUs), expanded uses of the technology, or requests for access**—whether from City of Seattle departments or external agencies—will undergo a **formal review and approval process**. This process will ensure:

- **Compliance with applicable laws and regulations**, including data privacy and public records laws.
- **Alignment with SPR's mission and policies** regarding security and public safety.
- **Proper protocols for storage, access, and data retention**, ensuring that only authorized personnel handle the information.
- **Appropriate safeguards** are in place to prevent unauthorized access, misuse, or improper disclosure of data.

All information-sharing requests will be **reviewed by the appropriate SPR leadership, legal counsel, and the Facilities, Access, Automation, Security Systems, and Technology (FAST) unit** before approval. Additionally, any future modifications to access policies or data-sharing agreements will be documented and reviewed periodically to maintain compliance with evolving legal and ethical standards.

6.5 Explain how the project/technology checks the accuracy of the information collected. If accuracy is not checked, please explain why.

The **Facilities, Access, Automation, Security Systems, and Technology (FAST) unit** within Seattle Parks and Recreation (SPR) is responsible for evaluating the **accuracy and relevance** of data collected by the FlashCAM system. The FAST unit will review all captured images and determine whether they pertain to **theft, vandalism, graffiti, illegal dumping, or other criminal activities** occurring on SPR property.

To maintain data accuracy and integrity, the following steps will be taken:

- **Review and Validation:** FAST unit personnel will examine captured photos to ensure they depict relevant incidents. Any images that do not contain evidence of unlawful activity will be promptly **deleted** in accordance with SPR's retention policies.
- **Compliance with Policies and Procedures:** The unit will follow established SPR policies and procedures to ensure that the information collected is **accurate, relevant, and lawfully retained or disposed of**.
- **Minimization of Unrelated Data:** If the system captures images of persons, vehicles, or activities **unrelated to the intended monitoring purpose**, those images will be **redacted, cropped, or deleted** to protect privacy and prevent the retention of unnecessary data.
- **Periodic Audits:** SPR will implement **periodic audits** of the FlashCAM system to ensure that data accuracy standards are upheld and that **improperly collected data is disposed of** in compliance with legal and department policies.

By implementing these safeguards, SPR ensures that only **accurate and relevant data** is retained and used for enforcement or investigative purposes while protecting individual privacy and maintaining compliance with applicable regulations.

6.6 Describe any procedures that allow individuals to access their information and correct inaccurate or erroneous information.

Individuals seeking access to their information or requesting corrections to inaccurate or erroneous data may do so through the **City of Seattle's Public Disclosure Request (PDR) process**. This process ensures transparency and allows individuals to review any records that may pertain to them, subject to applicable **privacy laws and exemptions**.

To request access or corrections, individuals may:

1. **Submit a Public Disclosure Request (PDR):** Requests can be made through the **City of Seattle's Public Records portal** or by contacting the designated public records officer within Seattle Parks and Recreation (SPR).

2. **Review Available Information:** If a request is approved, individuals will be provided with **accessible and releasable records** in accordance with **Washington State Public Records Act (RCW 42.56)**. Certain exemptions may apply to protect **privacy, law enforcement investigations, or other sensitive information**.
3. **Request Corrections:** If an individual believes the information captured is **inaccurate or erroneous**, they may request a **review and correction** of the record. The **FAST unit** within SPR will evaluate the request, determine the validity of the claim, and take appropriate action, such as **redacting, correcting, or removing inaccurate data** in compliance with department policies and legal requirements.

SPR is committed to ensuring that all collected data is **accurate, appropriately retained, and managed in accordance with City policies and state law**, while also protecting individual privacy rights.

7.0 Legal Obligations, Risks and Compliance

7.1 What specific legal authorities and/or agreements permit and define the collection of information by the project/technology?

The **Seattle Municipal Code (SMC)**, the **City of Seattle's Data Privacy Ordinance**, and other **City ordinances** grant the **Superintendent of Seattle Parks and Recreation (SPR)**, or their designees, the **legal authority to establish, update, and implement policies** related to the **use of technology for security, asset protection, and public safety**. These policies may be enacted **with the approval of the City Council and/or the Mayor's Office**, depending on the scope and impact of the policy changes.

Under the authority provided by the **SMC**, SPR is authorized to **collect and manage data** to:

- **Protect City assets** from theft, vandalism, graffiti, and illegal dumping.
- **Ensure public safety** and security within parks and recreational facilities.
- **Maintain the accessibility, integrity, and enjoyment of public spaces** within the corporate limits of the **City of Seattle**.

SPR's data collection practices will comply with the **City of Seattle's Data Privacy Ordinance**, which establishes guidelines for **responsible data collection, use, storage, and sharing** to protect individual privacy. SPR will align with **City privacy policies, state laws, and any future ordinances** that govern the **management of collected information**.

Additionally, SPR will develop **internal policies and procedures** to ensure compliance with **legal requirements, privacy protections, and data security standards** while safeguarding **public privacy and civil liberties**.

7.2 Describe what privacy training is provided to users either generally or specifically relevant to the project/technology.

Personnel within the **Facilities, Access, Automation, Security Systems, and Technology (FAST) unit** at **Seattle Parks and Recreation (SPR)** are required to complete the **City of Seattle's Annual Privacy & Security Awareness Training**. This training ensures that all staff handling data and technology are aware of **privacy laws, security protocols, and best practices** for managing sensitive information.

In addition to meeting **City of Seattle privacy requirements**, the **FAST unit** adheres to **State and National Standards** related to the **implementation and responsible use of new technology**.

To further strengthen compliance and accountability, **SPR is developing a comprehensive policy** that will govern:

- **Acceptable use of the FlashCAM system**
- **Photo retention, storage, and deletion practices**
- **Protocols for sharing records with law enforcement and other entities**

As part of this policy, **all personnel authorized to access or manage data collected by the FlashCAM system will receive additional training** specific to its operation, data security, and compliance with legal and privacy standards.

7.3 Given the specific data elements collected, describe the privacy risks identified and for each risk, explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Privacy Risks and Mitigation Measures

Seattle Parks and Recreation (SPR) has identified several **privacy risks** associated with the collection of data through the **FlashCAM system**. The department has implemented **strict policies and safeguards** to mitigate these risks and ensure compliance with **privacy regulations**.

1. Risk: Unauthorized Access to Data

- **Mitigation:** Access to FlashCAM data is **restricted exclusively** to the **Facilities, Access, Automation, Security Systems, and Technology (FAST) unit**. Data is stored on a **secured City of Seattle server or drive**, accessible only to authorized personnel. Additionally, **Executive leadership and HR** may view footage via a **secured, non-downloadable link** to prevent unauthorized sharing or distribution.

2. Risk: Retention of Unnecessary or Unrelated Data

- **Mitigation:** Any **photos or footage that do not capture theft, vandalism, graffiti, illegal dumping, or other criminal activity** are **immediately deleted** upon review by the FAST team. Additionally, regular **camera inspections** ensure that **unrelated activities, persons, or vehicles** are **permanently deleted** from the system.

3. Risk: Potential Exposure of Non-Involved Individuals or Private Property

- **Mitigation:** SPR follows **strict redaction protocols** to ensure that any **unrelated individuals, vehicles, or private properties** captured in images are **redacted, covered, or cropped** before storage or potential sharing with law enforcement. Cameras are **strategically positioned** to capture **only SPR property and areas with limited public access** while **masking adjacent private property** to avoid unnecessary surveillance.

4. Risk: Misuse or Overreach in Data Collection and Sharing

- **Mitigation:** SPR is **developing an official policy** to govern the **use, retention, and sharing of data** collected by the FlashCAM system. This policy will outline **acceptable use cases**, restrictions on **data access**, and guidelines for **sharing information with law enforcement**. The policy will also align with **Seattle's Data Privacy Ordinance** and any relevant **state or national standards**.

5. Risk: Lack of Public Awareness About Data Collection

- **Mitigation:** SPR will place **clear signage** at all monitored locations to inform the public that **FlashCAM surveillance is in use**. The signage will provide **transparency** about the system's purpose—**detering and documenting illegal activities such as theft, vandalism, graffiti, and dumping**.

By implementing these **privacy safeguards**, SPR ensures that data collection remains **limited, secure, and compliant with legal and ethical standards** while balancing **public safety and privacy concerns**.

7.4 Is there any aspect of the project/technology that might cause concern by giving the appearance to the public of privacy intrusion or misuse of personal information?

Yes, certain aspects of the **FlashCAM system** may raise **public concerns** regarding **privacy intrusion or potential misuse of personal information**. To address these concerns, **Seattle Parks and Recreation (SPR)** has implemented **clear policies, safeguards, and transparency measures** to ensure responsible use of this technology.

These measures include the feature that ensures **FlashCAM is only activated by motion and does not record live video**. Additionally, members of the public may worry that their **personal images or activities** could be **captured, stored, or shared inappropriately**.

To mitigate these concerns, SPR has established the following **privacy protections**:

- **Strategic Camera Placement:** Cameras are installed only in areas with **limited public access**, strictly monitoring **parks property** and avoiding surveillance of **adjacent private property**.
- **Limited Data Collection:** FlashCAM is **only triggered when motion is detected** and will not store any images unless an individual or vehicle remains after **the initial warning message**. If no illegal activity occurs, **no photos are taken**.
- **Strict Data Retention and Deletion Policies:** Any images that do not capture **theft, vandalism, graffiti, illegal dumping, or other criminal activities** will be **immediately deleted**. Additionally, individuals and vehicles **not involved in illegal activities** will be **redacted, cropped, or covered** to further protect privacy.

- **Public Transparency:** Clear **signage** will be placed in visible areas **notifying the public** that FlashCAM technology is in use.
- **Access Controls and Security:** Only authorized personnel within **SPR's Facilities, Access, Automation, Security Systems, and Technology (FAST) unit** can access the data, and all stored photos are secured on a **City of Seattle-approved server**.

By implementing these safeguards, SPR ensures that the **FlashCAM system** serves its **intended purpose**—to deter and document **illegal activities**—without compromising **public trust, privacy, or civil liberties**.

8.0 Monitoring and Enforcement

8.1 Describe how the project/technology maintains a record of any disclosures outside of the department.

Seattle Parks and Recreation (SPR) maintains a **strict record** of any disclosures of **FlashCAM data** outside the department to ensure **accountability, transparency, and compliance** with legal requirements.

All disclosures to **external entities**, including law enforcement agencies, the City's Law Department, or the general public, must be **formally processed and approved** by SPR's **Public Disclosure Officer** in accordance with the **City of Seattle's Public Records Act and Data Privacy Ordinance**. This ensures that all shared data complies with **privacy laws, retention policies, and security protocols**.

To maintain a **detailed record of disclosures**, SPR will implement the following procedures:

- **Documentation of Requests:** Any request for access to FlashCAM data will be **logged and reviewed** to determine if disclosure is legally permitted.
- **Approval and Authorization:** Before releasing any data, the **Public Disclosure Officer** will evaluate whether the request meets the **legal and policy requirements** for data sharing.
- **Audit and Compliance Tracking:** A **record of all disclosures**, including the **requesting entity, purpose of request, and date of disclosure**, will be maintained to ensure transparency and compliance with **City and State regulations**.
- **Protection of Non-Relevant Data:** Any **shared data** will undergo **redaction** to protect the privacy of individuals **not involved in illegal activities** before release.

These safeguards ensure that **FlashCAM data** is only disclosed **when necessary, appropriate, and in alignment with City policies**, while maintaining **public trust and privacy protections**.

8.2 What auditing measures are in place to safeguard the information, and policies that pertain to them, as well as who has access to the audit data? Explain whether the project/technology conducts self-audits, third party audits or reviews.

During the **pilot phase** of the FlashCAM program, Seattle Parks and Recreation (SPR) will collect **data and photos** while simultaneously **developing policies** related to **disclosure**,

tracking, and retention of information on theft, vandalism, graffiti, and illegal dumping. These policies will be incorporated into **SPR's official policies, procedures, and operating guidelines** to ensure compliance with **privacy and security standards**.

Auditing Measures

To safeguard collected data and ensure **accountability**, SPR has implemented the following **auditing measures**:

- **Self-Audits:** The **Facilities, Access, Automation, Security Systems, and Technology (FAST) unit** within SPR, which owns and operates the equipment, will conduct **regular self-audits** to monitor compliance with **data retention and privacy policies**.
- **System Monitoring and Access Control:** **Audit logs** will track **who accessed the data, when, and for what purpose**, ensuring transparency and security. Only **authorized FAST unit personnel** will have access to audit data.
- **Equipment Handling:** If technical issues arise with the FlashCAM system, the device will be returned to the vendor **without** any photos or captured data, ensuring that no sensitive information is inadvertently shared.
- **Annual Training Requirement:** All personnel involved in operating or accessing the technology will be required to complete the **City's Annual Privacy & Security Awareness Training**, reinforcing best practices for **data protection and compliance**.

These measures ensure that data collection, storage, and disclosure remain **secure, transparent, and aligned** with the **City of Seattle's Data Privacy Ordinance and relevant legal frameworks**.