BES: Mobile Security Observation Trailers

Privacy Impact and Risk Analysis

Draft revision agency

Smart City PDX

12/10/2024

PRIVACY ANALYSIS REPORT

City of Portland Privacy Toolkit

WHAT IS PRIVACY RISK AND IMPACT ANALYSIS?

The Privacy Impact Analysis (“PIA”) is a method to quickly evaluate what are the general privacy risks of a technological solution or a specific use, transfer, or collection of data to City bureaus or offices. The PIA is a way to identify factors that contribute to privacy risks and lead to proper strategies for risk mitigation or alternatives that may even remove those identified risks.

The Privacy Impact Analysis may lead to a more comprehensive Impact Assessment and a Surveillance Assessment depending on the level or risks identified and the impacts on civil liberties or potential harm in communities.

In the interests of transparency about data collection and management, the City of Portland has committed to publishing all Privacy Assessments on an outward facing website for public access. PIAs do not include specific uses of technology or data other than those initially evaluated.

WHEN IS PRIVACY IMPACT ANALYSIS RECOMMENDED?

A PIA is recommended when:

- A project includes surveillance technologies.
- A project, technology, data sharing agreement, or other review has been flagged as having some privacy risk due to the collection of private or sensitive data.
- A technology has high financial impact and includes the collection, use or transfer of data by city bureaus or third parties working for or on behalf of the city.

WHAT IS INCLUDED IN A PRIVACY IMPACT ASSESSMENT?

City staff completes two sections included in a privacy impact assessment report:

- *The Privacy Analysis form.* This document identifies all important information related to the project description, data collection, use, safekeeping, and management; as well as a verification of existing privacy policies and measures to protect private information.
- *The Privacy Risk Assessment.* This document breaks the privacy risk into six different areas of evaluation: (I) Individual Privacy Harms; (II) Equity, Disparate Community Impact; (III) Political, Reputation & Image; (IV) City Business, Quality & Infrastructure; (V) Legal & Regulatory; and, (VI) Financial Impact. Then compares risks to the likelihood of happening to create a single risk measure based on the worst-case scenario.

Executive summary

This privacy impact assessment supports the procurement process for mobile comprehensive security technology systems to monitor locations, deter crime, and notify designated City personnel when a security event occurs.

The comprehensive security system can include multiple types of cameras and sensors. This PIA focuses on pan-tilt-zoom, infrared and thermal cameras, panoramic field of view, and automatic detection features of people, animals, and vehicles.

This assessment has found the worst-case scenario brings a MEDIUM risk level.

Most risks derived from the collection of information more than necessary, including personal information for identification or license plate numbers. Risks also come from holding unnecessary footage too long, unauthorized access to footage and potential information breaches, unauthorized sharing, risk of chilling effects, risk of monitoring specific groups, and the risk of over surveillance.

The main recommendations to reduce identified risks include reducing cameras field of views to the minimum area of coverage, system access limitation, setting limits on sharing, only collecting necessary footage and minimizing retention periods, blurring faces where appropriate in public releases, and increase trust by informing the public and obtaining community input.

Risk area	Risk level	Highlighted risks
Individual Privacy Harms	Medium	1.1 The cameras will collect more information/footage than necessary to accomplish the purpose of monitoring the City's facilities.
Equity, Disparate Community Impact	Medium	2.2 Use of security cameras to monitor or surveil specific groups or people activity in the public realm.
Political, Reputation & Image	Medium	3.2 Lack of public information informing about the use of these security systems.
City Business, Quality & Infrastructure	Medium	4.1 Risk connected to mischaracterization or misidentification of contextual features in video footage.
Legal & Regulatory	Medium	5.2 Video footage is not properly anonymized.
Financial Impact	Medium	6.3 Risk of additional charges due to unplanned additional memory storage

Privacy Analysis

Purpose of the technology, project, data sharing or application

This initiative aims to implement a comprehensive security technology system throughout bureau-owned properties. The technology enhances our business continuity plan and meets the security needs of our community by deterring theft and vandalism, mitigating criminal activity in remote locations lacking physical security presence, and ensuring the safety of our staff and equipment. Mobile security trailers will be placed on Bureau of Environmental Services facilities like treatment plants and pumping stations. These trailers will not obstruct or interfere with pedestrian trails or public right of way. These devices are connected using cell networks and are designed to be both energy-efficient and environmentally friendly, as they are powered by solar energy and seamlessly integrate with the Genetec security access controls and video platforms.

Since 2022, the City has been participating in a pilot program using several unmanned mobile security units at various City sites. The pilot has proven to be successful in lowering the instances of security concerns at the locations of the unit deployments. There have been zero security breaches, theft, or vandalism to the City's critical infrastructure where these units have been deployed. The units have actively identified 1,242 potential security events throughout the life of the pilot enabling security personnel to be notified and investigate further.

Name of the entity owner of the application and website

Bureau of Environmental Services (BES)/ Bureau of Technology Services (BTS)

Type of Organization

City agency

Scope of personal data collected. List all sources of data and information.

Depending on the field of view of the cameras, footage could capture private property or public spaces where individuals travel through. Most footage will be of City infrastructure.

How personal data is collected.

Security cameras and additional sensors, including thermal images, infrared, and microphones, on the trailer will collect footage, potentially containing personal data.

Equipment description:

- Include 70-120 high resolution horizontal Field of View (FOV) or greater.
- Include optical, IR illumination, thermal and PTZ capabilities
- Include human, animal and vehicle detection within 650ft
- Include a minimum 58° (PTZ) and 360° (panoramic) horizontal FOV per camera
- Satisfy NDAA and TAA compliant options
- Be Federal Communications Commission (FCC) compliant

- Units must be equipped with tamper and intrusion detection capabilities to prevent theft or damage to the units. Tamper and intrusion detection capabilities are defined as automatic visual monitoring along with verbal notifications to discourage unauthorized access or damage.
- Include infrared and thermal capabilities for night and inclement weather
- Preferably have customer-configurable unit heads and mounting options
- Must have the ability to disable facial recognition

Who can access the data?

The Bureau of Environmental Services (BES) security team will have access to alerts, notifications, and footage collected by the security trailer. The BES Security Manager will be responsible for these devices. Vendor staff may have access to maintenance or equipment management tools.

Purposes the data is used for

Using surveillance technology, proprietary software and hardware for mobile, cloud-based security solution. The units are solar powered and connected using cell networks. Mobile security trailers will be placed on Bureau of Environmental Services facilities like treatment plants and pumping stations. These trailers will not obstruct or interfere with pedestrian trails or public right of way.

The City has many capital infrastructure facilities throughout the City including over a hundred pump stations, green spaces, labs, pools, parking lots, etc. Since the COVID Pandemic, the City, like many other organizations, has seen a significant increase in theft, vandalism, and personnel safety concerns.

These security cameras systems can offer a flexible solution to the protection of City infrastructure and employees. The main function of these units will be to monitor specific locations, deter crime, and notify designated City personnel when a security event occurs.

The data will be used for surveillance purposes. Because of the importance of critical infrastructure, BES needs a security technology solution to prevent and limit any downtime. If criminal activity is captured, footage data will be used for investigations or judicial proceedings.

These security systems will support:

- Security force and alerting multiplier
- Meets operational continuity strategies
- Deter theft and vandalism
- Prevent thefts and other crimes at remote locations
- Protect staff & equipment
- Uninterrupted service & immediate notifications
- Security bang for the buck

- Self-sustaining mobile platform with no need to be supported or maintained by the Bureau of Environmental Services (BES) IT and/or the Bureau of Technology Services (BTS) resources. The vendor will provide maintenance of the entire mobile platform.
- Off-the-grid operation.
- Integrate with BES' Genetec security solution

Where the data is stored

Video footage and other sensor information is stored first in the units and sent to the vendors cloud servers. Copies of footage from relevant or potential criminal activity events can be transferred to City's storage for analysis or trigger a security action.

How data is shared

Data sharing is case dependent. In cases where criminal activity occurred, footage will be shared with the Portland Police Bureau. Records of footage access and sharing could be accessed by City staff and supervisors to monitor any potential unauthorized access or information breach. Otherwise, footage will not be accessible to any other individual or team.

How long is the data stored?

Access to video footage is limited to those that need to manage and supervise the security units, and all access is logged. Footage and sensor data can be shared with law enforcement in cases of an incident or crime.

The vendors may store video footage locally until it is pulled into their cloud storage platform when requested by the customer as they view a specific segment of video. Video footage is then stored in the vendor's cloud storage until the customer deletes it.

On the City side, different retention schedules may apply to footage depending on whether it recorded actions involved in property damage or any other criminal activity. Vendors should comply with public records retention schedules.

Public records include those that are used by the City. State public records requirements apply to the City.

https://www.portland.gov/archives/retention-schedules
Facilities Operations FCO-0020 - Video Surveillance Recordings
(a) 30 days for regular recordings; (b) If used in grievance, investigation, or incident report, retain until the resolution or disposition of the case.

Administrative ADM-0450
Retention schedule for Photographs, negatives, slides, digital, and moving images documenting City projects, activities, events, properties and responsibilities.

Administrative - ADM-0570
Property Damage Records - If not litigated, retain 3 years after the date of last action; if litigated, coordinate with the City Attorney's Office. It may contain confidential information.

https://oregon.public.law/rules/oar_166-200-0390
ORS 166-0390(5) Property Damage Records — Minimum retention:
(a) If litigated, see Civil Case Files in the Legal section for retention.
(b) If not litigated, retain 3 years after the date of last action.

Effectiveness

Vendor and devices technical specifications dependent. As different vendors offer different kinds of cameras, audio recording devices, and speakers the effectiveness of each vendors hardware or software cannot be analyzed.

Security systems are used to assist City property and personnel protection. These cameras monitor areas of interest, and the collection of moving images and other sensor recordings are downloaded only when incidents have been identified. This information triggers specific security actions.

CCTVs or Closed-Circuit TV cameras are used for various reasons: to keep property safe and secure for employees; to provide a cost-effective method to monitor a location, provide archived video coverage for investigations; and to deter future crime or attacks, such as robbery, burglary or vandalism.

Crimes in progress may be detected and possibly prevented since the video feeds can be monitored in real-time. Also, a clearly visible camera alerts the public that they are being monitored, which may deter criminal activity.

Networked security video systems typically consist of analog or IP cameras, recording devices, and monitoring capabilities with a network consisting of closed-circuit video cameras, video recorders, and monitoring capabilities that captures video-only feeds or a stand-alone system with one camera monitoring a specific area. The cameras are capable of streaming live video shots but most of the government networks of security video systems use firewalls to limit viewing to those in the viewing room or to those viewing through remote monitoring.

The CCTV cameras include a series of fixed cameras and pan-tilt-zoom (PTZ) cameras. Some cameras used for CCTV systems utilize zoom capability with manual tracking (i.e., panning and tilting), which allows the officer conducting the monitoring to gain the best image of any activity. Some CCTV systems can be set to automatically tour an area. The cameras are placed in various locations on the perimeters or inside of BES facilities, such as water treatment plants or remote pumping stations.

Cameras contain low-light technology to support detection of unauthorized or suspicious activities at night.

This security camera system could be installed close to access points, designated entrances, and secured areas, to provide the greatest possible range and area of monitoring.

The cameras should not be placed in areas with a reasonable expectation of privacy like viewing into private property, bathrooms or changing rooms. Footage of passersby or overviews of private property with no connection to any incident should be discarded immediately.

The City will use the video feeds to detect and respond to potentially unlawful activities in real time in the areas using CCTV. The video feeds may also be used to support law enforcement investigations to the extent that they contain information relevant to a criminal (or potential criminal) activity.

Privacy protections for CCTV systems include limiting access to the video feed to only authorized personnel and law enforcement agencies, establishing clear auditing systems so every use of the CCTV system is logged and reviewable and restricting storage to six months or less.

City employees could be subjected to administrative actions if any misuse occurs in conformity with existing Human Resources rules, laws, and regulations.

Proportionality and Necessity

PROPORTIONALITY

The purpose of the camera network is to protect city infrastructure and community investment. A camera system allows for 24/7 coverage of critical infrastructure. Multiple cameras could be used such as a high resolution horizontal FOV camera, Pan Tilt Zoom Camera, 360 Panoramic Camera, Forward Looking Infrared Camera to perform this function.

Not surveilling infrastructure could expose it to theft and other harmful events. Most camera systems monitor large areas around security trailers. The trailers are on city owned lands and will collect largely public information. Depending on the location of the trailers, cameras could capture video and audio from private areas. Avoid using cameras to actively surveil via livestream for crimes unrelated to critical infrastructure.

Surveillance does not necessarily equate to protection. The data collected will help protect infrastructure and people, if it notifies security quickly enough to intervene. The bureau will assign a team to monitor live video feeds, and some vendors may offer automatic features that support this task. There will be mechanisms that trigger a protective response. Without the protective response, the surveillance alone will indirectly protect infrastructures by deterring crime and collecting data for reprimand.

There are potential alternatives to live stream or using multiple types of cameras, for example, decoy cameras can deter threat actors without surveilling (i.e., collecting information) while covert surveillance cameras won’t do much for deterrence but the data it collects will be useful for reprimand and response.

Alternatives to surveillance cameras will stem from the category of things stopping threat actors from physically entering restricted areas (i.e., prevention and response) such as fences, locks, signs, security guards, police response, etc.

Privacy and security may seem like opposites but there is a way for there to be high security and high privacy. Unfortunately, high privacy and security in this case may be too expensive (e.g., 24/7 security teams at each site). It is also possible to have low security and low privacy, where there is surveillance but few ways to protect sites, preventing theft or other harmful events. The project is in the middle. It is better to approach high security and high privacy, nevertheless, by deploying privacy controls.

The trailer’s flashing lights and its display of cameras will deter would be threat actors. Flashing lights and loud voices and noises may have unequitable impacts to people with disabilities or mental health sensitivities. In the case of a threat event, the City could use the data as evidence. The camera system used to secure critical infrastructure creates risks, but if data collection is limited, and if the camera system and data are used “defensively” then the project is worthwhile.

Commented [GA1]: See email for details - ADA/ Accessibility concern (unequitable Impact)

Commented [HD2R1]: Added a sentence in this paragraph.

Compare this to a camera system that generates more harm than if there were no camera system by also surveilling the surrounding area indiscriminately. If data processing is limited to the sub-goals that fall under security, such as deterrence of, response to, or reprimand of threat actors on critical infrastructure, then technology and data may be considered proportional to the goals of the project. Surveillance should be in public’s interest without being an imminent threat to the public’s rights.

If restricting the angles of rotation of the camera or technically blurring portions of the camera’s field of view cannot be done, it may be worth looking into alternatives that could offer security without the additional privacy risks. The collection of video and audio data from private areas (e.g., backyards, sides of houses) may be an intrusion on seclusion, despite data retention time limits or sharing limits.

Commented [GA3]: Is there a method for review or relocation of surveillance devices if someone objects to a location (eg, if it is recording into their backyard and they're uncomfortable, etc)

Commented [HD4R3]: We can add it to the risk mitigation strategies.

Commented [HD5R3]: Added to risk 1.7. mitigation e.

The City should also be wary of instances where surveillance undermines the interest in which it is supposed to protect, that is, the security of critical infrastructure and the well-being of the community. [1] For example, if we enable surveillance for other crimes unrelated to the protection of critical infrastructure such as speeding, parking violations, jay walking, people or workers may avoid the view of the observation trailer increasing the risk of crime in these out of sight areas. Or if someone determined that these security trailers protect something valuable, the blue strobing lights that were a deterrent could be targets, although this is unlikely. These lights may have unequitable impact on photosensitive individuals and people with certain ADA requirements.

Commented [HD6]: @Mares, Cesar I wonder if we can think about examples.

Commented [MC7R6]: something like these two examples. Clarissa Veliz mentions this idea in her book "the ethics of privacy and surveillance"

Commented [MC8R6]: i have the "conspiracy theory" hat on so i wouldn't mind deleting the paragraph

Commented [HD9R6]: Thank you Cesar. I think these examples provide a good idea of the effectiveness of the technology.

Commented [GA10]: See email for details - ADA/ Accessibility concern (unequitable Impact)

Commented [HD11R10]: Added risk 2.4

[1] https://www.tandfonline.com/doi/full/10.1080/2573234X.2021.1920856#d1e233
Véliz, Carissa. *The Ethics of Privacy and Surveillance*. Oxford University Press, 2024.

NECESSITY

Although technology is not necessary to complete the purpose of the project, it is necessary to complete the purpose of the project effectively given the project’s scope. Because the intended purpose is to provide security for these important areas 24/7, 365 days out of the year in case of a low probability but highly impactful event, employing a fleet of security individuals is less effective and more costly than deploying the camera system that would notify security individuals or perform some other protective response.

Commented [HD12]: @Mares, Cesar This assessment could help with the discussion of privately owned security cameras looking at public spaces.

Commented [MC13R12]: I'll keep that in mind. I didn't know it could have that effect.

Current Privacy Safeguards

1. Limits on Access. Data analytics of observation trailers, live monitoring, are only available to security personnel.
2. Limit on Data Retention set at 30 days, unless data is needed for investigations.

Open source

No

AI/ML claims

Likely, depending on the vendor’s offer.

Privacy Policy or relevant laws(link)

Vendor dependent.

Privacy risk

Medium. Some risks need to be mitigated.

Surveillance Technology?

Yes.

Portland Privacy Principles (P3)

Data Utility*: All Information and Data processes must bring value to the City of Portland and the communities the City serves. The City will collect only the minimum amount of Personal Information to fulfill a well-defined purpose and in a manner that is consistent with the context in which it will be used.*

Protecting critical infrastructure is important and valuable. All technology and data oriented toward this aim will bring value to communities directly and indirectly. It will bring value Indirectly through the technology’s effect on infrastructure security and directly by providing surveillance for personnel around these sites. Granted that the suggestions on field of view restriction are adopted and suggestions involving proportionality, the technology and the data it collects will be aligned with the principle of Data Utility.

Full Lifecycle Stewardship: *Data, Metadata and Information will be secured and protected throughout its life cycle.*

All cybersecurity and information security procedures the city complies with regarding other technology will apply and be upheld with this technology, including but not exhaustively, encryption and secure passwords. [2]

Transparency and accountability*: How the City uses, manages and collects information is described clearly, accurately, and shared in an accessible way. Who creates, contributes to, and has access to that information is also clearly documented and communicated to all people who entrust city government with their data and information.*

Observation trailer towers will have blue strobing lights indicating its presence. Aside from providing notice, the current state of the project aligns with the principle of transparency and accountability. There is a security team with specific duties. Documentation about security events and logging data sharing could be actionable mechanisms for transparency.

Ethical and Non-Discriminatory Use of Data*: The City of Portland has an ethical responsibility to provide good and fair stewardship of data and information, following existing non-discriminatory protections, and commits due diligence to understand the impacts of unintended consequences.*

The City plans to use video and audio recordings for protective purposes. The data will be handled using standard cybersecurity protocols. Decision made from the data will be for protective responses or reprimand.

Data Openness*: Data, metadata and information managed by the City of Portland -- and by third parties working on behalf of the City -- that are made accessible to the public must comply with all applicable legal requirements and not expose any confidential, restricted, private, Personal Information or aggregated data that may put communities, individuals, or sensitive assets at risk.*

There won't be an open data aspect in this project.

[2] https://www.portland.gov/policies/technology-services/information-security/bts-201-information-security-administrative-rule

Equitable Data Management: *The City of Portland will prioritize the needs of marginalized communities regarding data and Information management, which must be considered when designing or implementing programs, services, and policies.*

The value of the project is roughly equally distributed, but the downsides still need to be accounted for and analyzed for unequitable distribution of harm.

Automated Decision Systems

Commented [MC14]: Am i missing anything?

Commented [HD15R14]: I think this paragraph can go.

There are additional concerns about the ground truth validation of these algorithms and built-in safeguards. The lack of algorithmic audits and certifications make hard to vet vendors offers of artificial intelligence features until they are used in practice.

Privacy Impact Risk Severity Assessment

WORST CASE SCENARIO	**MEDIUM**

Baseline (B): (T) – Technology level, (U) – use and application level.

Risk type (RT): (I) Individual Privacy Harms; (II) Equity, Disparate Community Impact; (III) Political, Reputation & Image; (IV) City Business, Quality & Infrastructure; (V) Legal & Regulatory; and (VI) Financial Impact.

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
U	I	1.1 The cameras will collect more information/footage than necessary to accomplish the purpose of monitoring the City's facilities.	Moderate	Likely	This risk is connected to what the security cameras can access in their field of view and whether they can record activities happening in the public realm or private property. This could lead to unnecessary footage recording of private activities. Footage is constrained to the BES security team and shared to law enforcement when incidents are identified. Footage is also accessed due to FOIA requests. In this case, any person's face should be blurred or anonymized. Different camera types may have different mitigation strategies. For fixed cameras, verify location and that the field of view minimizes any public or private spaces. Center the view to those areas of interest within BES property. Inform the public, particularly any neighbor house or property about the purpose of the security cameras, informing about the potential impacts and benefits. Try to capture and release a sample of the camera's field of view to assure neighbors what it is seen.	Medium

					The following is an overview of the cameras used in security mobile systems. All these cameras should follow the general mitigation recommendations in this assessment. 1) 70-120° or greater high resolution horizontal FOV (Field of View) Camera is focused to a specific area of interest and may include sections of the public realm or private property. These cameras should minimize the unnecessary collection of footage not involving an incident of interest. 2) PTZ (Pan-Tilt-Zoom) cameras can change the field of view at command and have extended field of view. Minimize the exposure to non-City property, as it is understood that in certain cases it would be necessary to pan and cover areas where potential criminal activity may be happening within the City's property. Inform the public about the practices using this type of cameras. 3) 360° (panoramic) horizontal FOV (Field of View) Camera collects a large area and may include adjacent private properties and the public realm. Images from these cameras are usually not in the highest resolution due to their large field of view, but they could still collect people's faces and their activities. 4) FLIR (Forward Looking Infrared) cameras use thermographic images from the emission of infrared light. These images are already obscured, and identification is unlikely. These cameras can be used to distinguish a person from an animal and any heat-emitting devices. These cameras have low privacy risks in general. The FLIR camera system can pose additional concern to the public about potential for privacy intrusion based on the	

					misconception that the camera can record people and objects inside homes and other structures. The FLIR camera in this system is not capable of looking through walls or structures. Any risk can be mitigated by informing the public about the sensors used and practices to protect privacy and individual rights.	
T	I	1.2 Risks of collecting private or personal information due to retention of unnecessary footage.	Moderate	Likely	Video feeds detect and respond to potentially unlawful activities in real time or to support law enforcement investigations and prosecutions to the extent that they contain information relevant to a criminal (or potential criminal) activity. It is expected that most of the video collected by the cameras is not relevant and becomes unnecessary to the goal of this system. All the cameras on a security trailer are initially stored video on board and not streamed up to the cloud until an incident has been detected. It is until a human operator retrieves the video after the system reports an incident triggered by presence sensors. The real time streaming and footage is reviewed to determine whether a real incident is or has happened. Storing unnecessary video footage may include individuals, including children, and activities not relevant to the purpose of this technology or even against the Oregon Law (ORS 30.831). These risks can be reduced by: a) Minimizing the access to video footage, particularly when no criminal activity or potential incidents are detected b) Provide proper training to operators on privacy protection and best practices in security under the Oregon Law. c) Reduce the retention time of non-relevant footage to a minimum.	Medium

					d) Train public records personnel to anonymize and blur a person's face in moving images	
T	I	1.3 Unauthorized access to recorded footage	High	Unlikely	Recorded footage gets stored in the cloud or copied in a City owned device. Unauthorized access is considered a privacy data breach and may trigger a deeper cybersecurity assessment. To mitigate individual privacy impacts the security team should: Follow cybersecurity and information protection best practices as described in the City'shttps://www.portland.gov/policies/technology-services/information-security Information Security Administrative Rules. Report any unauthorized access to the Information Security Office (BTS 2.08) Periodically review access log files to the security system Minimize the collection of footage to the required when a security incident is in progress. Train operators and security personnel in incident and privacy breach response	Medium
T	I	1.4 Personnel use cameras in unauthorized purposes	High	unlikely	The risk that personnel use cameras for other purposes than protecting City's facilities and personnel may result in privacy breaches and impact organizational reputation. Create a procedure to assess impacts of personnel using security equipment for other purposes. Train personnel about the responsibilities of using security equipment and impacts of unauthorized use of equipment. Create accountability measures that lead to corrective and remediation procedures. Follow existing Human Resources rules (HRAR-4.08 - Information Technologies).	Medium

					Report these incidents as privacy breaches and include the action taken for remediation	
U	I	1.5 Recorded footage is shared to unauthorized third parties.	High	unlikely	Footage may be shared to third parties intentionally or unintentionally. Third parties may include other bureaus, offices, jurisdictions, media outlets, private companies, or individuals. Third parties may reshared the information received publicly and create additional privacy harms and impacts to individuals and the City's reputation, which could end in litigation. To minimize unauthorized sharing of information to third parties follow these recommendations: a) Ask personnel to request authorization before sharing to third parties. b) Review protocols for protecting information and accessing services that allow viewing or downloading footage, incident data, and sensor information from the vendor's service site. c) Train personnel on responsible data and information sharing practices. d) Work with City partners to create joint information protection practices to allow information sharing. e) Report any unauthorized information sharing.	Medium
U	I	1.6 Risk of generating an oversurveillance environment in the community.	High	unlikely	Lack of public information about the implementation and use of surveillance and security equipment may lead to a sense of oversurveillance due to misinformation, or speculation about how the technology is used and for what purposes. This can be particularly impactful to specific groups and nearby neighbors. The risk can be mitigated by the publication of information about this technology and its purpose, including this	Medium

					assessment. This public information needs to make clear that City properties are under surveillance and why the cameras are necessary. On-site signs describing the use of surveillance cameras, purpose, agency responsible, access to additional information, and ways to provide feedback can enhance public trust and transparency. It is suggested to create public information on the web and periodically update it with incident reports and other performance metrics. This web page can include information about how the City is protecting neighbors and individuals' privacy.	
U	I	1.7 Risk of using live streaming features to monitor activities in the public realm or private property	Moderate	unlikely	Members of the public may be concerned that cameras are live streaming video, particularly if the perception of the camera's field of view includes the public realm (like streets, parks, or schools) or private property. To mitigate this risk: a) Limit the personnel with access to livestream video footage. b) Implement periodic revisions of activity logs to identify unauthorized use. c) Inform the public about the limitations and safeguards around live streaming video. d) Include information about the camera’s field of view in privacy assessments. e) Include a method or mean for review or relocation of the trailers or devices if a valid objection is received.	Low
T	I	1.8 Risk of recording private audio conversations.	Moderate	unlikely	These mobile security stations include a two-way speaker. The system can allow communication and record audio, potentially storing private conversation in the background not relevant to the operation of the security operations.	Low

					1. To mitigate this risk, only use the audio systems to the extent necessary to ensure proper security operations. 2. Do not record audio without the proper justification. 3. Immediately delete any unintentionally-recorded audio. 4. Recording audio conversation should be disabled. The unintentional recording of people's voices and conversations outside the context of a criminal incident could be considered an invasion to personal privacy. The recommendation is to minimize audio recording and train personnel on when not to record audio conversations. Best option is to disable audio conversation recordings.	
T	II	2.1 Use of security cameras may restrict freedom of speech or association.	High	rare	The system does not in any way restrict freedom of speech or association. The images are primarily used to detect and deter criminal activity. The images are not used to restrict or investigate lawful rallies and associations. The occurrence of First Amendment-protected activity, such as a protest or rally outside a City facility. Unless there is evidence of criminal activity that must be investigated or prosecuted, The City will not maintain those images for longer than the storage capacity. The City may share images only for legitimate law enforcement purposes or in response to public records requests. To mitigate this risk: 1. Train personnel involved in operating the cameras and managers in privacy protection practices, including civil liberties and civil rights 2. Improve transparency measures by promptly releasing incident metrics and sharing of information, particularly during protests or civil disobedient events.	Medium

					3. Work with City Attorneys and privacy experts to request literacy and training materials.	
T	II	2.2 Use of security cameras to monitor or surveil specific groups or people activity in the public realm.	High	unlikely	Besides protest and civil disobedience events around facilities, certain groups may feel specifically over-surveilled or monitored, including people experiencing homelessness, and Black, Indigenous, and People of Color residents. Inform residents about the purpose of the surveillance equipment by placing information about the equipment, its purpose, who owns it, and where to contact or how to request more information. This information should be visible to all from the public realm (adjacent streets or sidewalks). The perception that this security equipment will deter criminal activity can be validated by collecting the proper data and collaborating with Portland Police and other first responders. If possible, collect demographic information to assess whether impacts are happening more on specific groups. The agency should demonstrate and inform how the cameras are used in events like public demonstrations close to the City's facilities and focus on property and employee safeguarding.	Medium
T	II	2.3 Risk of public intimidation.	Moderate	Rare	The use of lights, loud alarms, and other means that deter unauthorized access to facilities or criminal actions may create an unintended intimidation or distressing environment to neighbors or by passers. People with mental health sensitivities or trauma may have lower thresholds to alarms and bright lights. To mitigate this effect, use these deterrent measures as the last defense. Informing neighbors and adding proper signs informing of actions and ways to provide public feedback to	Low

					improve relationships with neighboring properties and the public. These could be some effective ways to mitigate the risks outlined above: • Strobe lights could be removed or disabled. • Strobe lights occur on demand, caused by a human actor, only when a potential incident is observed. • If strobes are continuously flashing, only at locations that are substantially removed from routine paths of pedestrian transit and far away from any residences. • Strobes could be required to blink within a specified parameters for frequency and brightness, as outlined by the recommendations of the National Epilepsy Foundation, or similarly recognized institution: “Generally, flashing lights between the frequencies of five to 30 flashes per second (Hertz) are most likely to trigger seizures. To be safe, the consensus recommends that photosensitive individuals should not be exposed to flashes greater than three per second.” - source- National Epilepsy Foundation[3]	
U	II	2.4 Risk of unequitable impacts to individuals with ADA/Accessibility needs.	Moderate	Possible	If blue strobes are placed near to remote pedestrian or cycling trails, there is risk for the lights to induce medical episodes in places where help will be slow to arrive, if at all. (And outside of the view of the live-feed cameras, as the lights will be visible beyond the cameras’ range of view). Strobe lights occur on demand, caused by a human actor, only when a potential incident is observed. Trailers could be placed close to residences, where flashing lights would negatively impact quality of life and/or experience of being excessively surveilled. Blue strobe	Medium

[3] https://www.epilepsy.com/stories/shedding-light-photosensitivity-one-epilepsys-most-complex-conditions#:~:text=Generally%2C%20flashing%20lights%20between%20the,greater%20than%20three%20per%20second.

					trailers are being used in private parking lots to deter camping; there is a possibility that these trailers could be used in a similar “off-label” manner. If strobes are continuously flashing, only at locations that are substantially removed from routine paths of pedestrian transit and far away from any residences. Depending on the rate of the strobing light, it could cause harm to people with epilepsy. Strobes could be required to blink within a specified parameters for frequency and brightness, as outlined by the recommendations of the National Epilepsy Foundation. [4]	
T	III	3.1 Risk of impacts on the City reputation and image from overusing surveillance.	Moderate	unlikely	This risk may appear when a perceived failure in public trust appears. For instance, an information privacy breach or misused of equipment. Remediation of public trust is based on implementing transparency and accountability measures. Reduction of the likelihood of these risks is a result of avoiding misused and improving information protection and privacy safeguards. Transparency and accountability can be improved by informing the public about the purpose and limitations of the mobile security system and sensors on it. Information about privacy safeguards, number of incidents and how they are resolved, and periodic reports can improve public trust. It is also recommended to reach out to residents about the purpose of the technology, particularly around locations where facilities are close to residences or the risk of capturing footage of busy streets.	Low

[4] https://www.epilepsy.com/stories/shedding-light-photosensitivity-one-epilepsys-most-complex-conditions#:~:text=Generally%2C%20flashing%20lights%20between%20the,greater%20than%20three%20per%20second.

U	III	3.2 Lack of public information informing about the use of these security systems.	Moderate	Likely	Not informing properly about the use of these systems, particularly when they include multiple methods of footage collection and deterring methods, can create mistrust in the community and privacy advocates. The recommendation is to use publicly accessible signs that include descriptive information about the use of surveillance cameras, including purpose, description of technology, agency responsible for its use, and ways to provide input on their use.	Medium
T	IV	4.1 Risk connected to mischaracterization or misidentification of contextual features in video footage.	Moderate	Possible	This risk refers to the possibility of misidentifying an object, behavior, or a context that may lead to a false positive incident detection. False positive detection is when an incident is reported, but there is no real activity of interest. This may lead to wrongful detentions or unnecessary law enforcement activity. A City staff part of the agency or City security team will decide if an incident has happened or is ongoing. Even when multiple triggers are reported from the security system, a human operator must decide the thread level and the proper action. Mitigation strategies include: a) Proper training to operators, logging and record of incidents and their details, performance measures, and proper continuous improvement programs can help to reduce false positives and general effectiveness of the security system. b) Keeping proper equipment maintenance and working with the vendor to troubleshoot issues should reduce the likelihood for missing incidents.	Medium

T	IV	4.2 Incidents are not detected or missed (false negatives)	Moderate	Unlikely	A false negative incident is when an activity that should have been detected is not. A mobile security trailer has redundant sensors; however, poor lighting or environmental conditions like rain, snow, smog, etc. may create more difficult conditions for these systems. Also, the lack of maintenance, low power, particularly in wintertime, critters chewing on cables, vandalism, or the natural exposure to the environment may reduce equipment effectiveness. False negatives may end up with property damage, loss of goods in facilities, or even put personnel at risk. Mitigation strategies include: a) Provide required maintenance to equipment and work with the vendor to troubleshoot issues with the equipment. Report any issue to the proper group. b) Training personnel to identify issues and resolve them may save time and increase effectiveness of the cameras.	Low
U	IV	4.3 Risk of vandalism and extraction of footage directly from the mobile security unit.	Moderate	Unlikely	This risk emerges from the physical tampering of electronic devices and extracting local storage units. Most units should be designed robust enough to protect them from vandalism. In any case, footage should be stored encrypted.	Low
	IV	4.4 Risk of using unreliable or non-explainable Artificial Intelligence features.	Moderate	Possible	Using artificial intelligence (AI) features may create a false sense of security, particularly when decisions are fully automated. The agency needs to assure AI features are reliable and provide certain level of explainability. The agency needs to assess the levels of risks and impacts of decisions involving artificial intelligence features. High risk and high impact applications are encouraged to include trained staff to validate those decisions.	Medium

					Certain AI claims like emotion or behavioral identification should be disqualified at this point due to the lack of effectiveness, auditing services, and the high level of risks that false positives may create.	
T	V	5.1 Retention schedule is too long, increases the risk of unintended uses and impacts.	Moderate	Possible	Video surveillance recordings have a 30 days retention schedule if not used in grievance, investigation, or incident report, retain until the resolution or disposition of the case (ORS 166-200-0405). Public records include those that are used by the City. State public records requirements apply to the City. Since the City will be using these data, it's the City, not the vendors, who must retain it in compliance with the schedules. If the City can't compel the vendors to retain the data, the City will need to copy the data to its own servers. The City needs to comply with legal requirements for collecting footage involving property damage when there is no litigation involved. FOIA requests may make this footage available to the public and proper anonymization of individuals need to be included in the process. Failure to comply with either retention times or FOIA requests may result in litigation against the City.	Medium
T	V	5.2 Video footage is not properly anonymized.	High	Possible	Blurring faces and properly anonymizing individuals or sensitive information like license plates can be a tedious task and some automatic tools may fail to identify all faces and aspects of an individual that need to be anonymized. FOIA requests may include faces, children, and other vulnerable groups when the cameras include public spaces. To mitigate this risk, include proper training to operators in charge of responding to FOIA requests and include peer reviewers of assistant software for blurring faces.	Medium

					360 panoramic camera footage could be challenging for this type of software due to its distorted geometry. Human reviewers are encouraged. Reach out to the Public Records Office to learn about how to anonymize images.	
T	VI	6.1 Risks of property loss or damage due to faulty equipment	High	Unlikely	Faulty equipment may appear due to lack of maintenance or damage due to critters or vandalism. Ineffective or damaged equipment may lead to property loss or damage without fulfilling the equipment purpose. Mitigation strategies include: a) Mitigate financial impacts due to property damage, including the equipment itself, by protecting equipment with redundant systems, like alarms or other secondary security cameras that may provide information even when main systems are down. b) Periodically assess if the equipment is at risk. c) Provide training to security personnel on how to respond to attacks to critical infrastructure or equipment	Medium
T	VI	6.2 Risk of property loss or damage due to vandalism	Moderate	Rare	Equipment can be intentionally damage for different reasons and purposes. Assessing the risks of vandalism depends on how accessible to the public these devices can be and the type of facility where they have been installed. Signs informing people about the specific purpose and use of these device will inform most people and reduce the risk of vandalism. To improve device security, explore areas where cameras can be effective and reduce risks to have blind spots. Particularly when devices are installed in publicly accessible spaces with poor lighting. Repair any damage as soon as possible.	Low

U	VI	6.3 Risk of additional charges due to unplanned additional memory storage	Moderate	Possible	The accumulated footage may create additional storage needs that may pass basic services. The team needs to understand what the vendor’s storage are offer and costs attached to managing footage. Different strategies to store only events of interest may need to be better understood.	Medium
U	VI	6.4 Risk of additional charges due to AI services.	Moderate	Possible	Some additional services that may include artificial intelligence tools may require additional fees. The recommendation is to evaluate the use of AI tools including effectiveness, costs, and technical requirements and risks.	Medium

Appendix A
Privacy risk assessment framework

Severity (Evaluate for the worst / highest possible impact)				
	A: Low	**B: Moderate**	**C: High**	**D: Extreme**
Individual Privacy Harms	Customer or “telephone book” information collected and could be disclosed (excluding utility customer data, protected by RCW)	Potential disclosure would be limited to non-financial, non-health related information; no personal identifiers (e.g., social security and driver’s license #s)	Financial or other highly sensitive information would be collected and disclosable requiring action to remediate negative effects (example: non-HIPAA health data); i.e., credit report management required	Disclosure would result in extreme privacy impacts to highly regulated information; catastrophic public release of financial and personal information requiring credit report monitoring and other remediation
Equity, Disparate Community Impact	Little or no equity impact, technology delivered uniformly without reference to individuals or demographic groups	Accidental or perceived disparate impact to communities by nature of location of technology or service delivered	Intentional disparate equity impact resulting in community concern resulting in privacy harms, media coverage; loss of reputation, legitimacy and trust impacted	Extreme impacts to community, City experiences national media attention; widespread public concern and protest; significant breakdown in business processes associated with damage control
Political, Reputation & Image	Issues could be resolved internally by day-to-day processes; little or no outside stakeholder interest.	Issues could be raised by media and activist community resulting in protests and direct community complaints	Disclosure would likely result in heavy local media coverage; reputation, legitimacy and trust impacted	Likely national and international media coverage; serious public outcry; significant breakdown in business processes associated with mitigation and damage control
City Business, Quality & Infrastructure	Management of disclosure issues would represent negligible business interruption; resolved with no loss of productivity	Issue management would result in brief loss of services; loss of < 1 week service delivery; limited loss of productivity	Significant event; loss of > 1–3-week loss of services; critical service interruption to delivery of infrastructure services	Extreme event; business collapse for department services; loss of > = 3 months of data or productivity; critical business infrastructure loss > 1 month
Legal & Regulatory	Adverse regulatory or legal action not indicated or highly unlikely	Relatively minor incident, regulatory action unlikely; possible legal intervention or consultation for addressing data exposure or loss	Adverse regulatory action likely – i.e., fines and actions associated with CJIS, HIPAA, PCI, NERC, COPPA violations, etc.	Major legislative or regulatory breach; investigation, fines, and prosecution likely; class action or other legal action
Financial Impact	$0-$500 impact; internal costs covered, and no significant external costs incurred	>$500 - $5,000; internal and external costs associated with legal consultation, system rework, overtime	> $5,000 -$50,000 external costs associated with fines, consultation fees and regulatory actions to mitigate information exposure; internal costs associated with system rework, overtime	> $50,000 external costs associated with fines, consultation fees and regulatory actions to mitigate information exposure; internal costs associated with system rework, overtime

Likelihood analysis.

For assessing probability of risks

Likelihood	Probability
Almost certain	Likely to occur yearly
Likely	Likely to occur every 2 years
Possible	Likely to occur every 5 years
Unlikely	Likely to occur every 10-20 years
Rare	Has never occurred

Risk Matrix

	Low	**Moderate**	**High**	**Extreme**
Almost Certain	🟧	🟧	🟥	🟥 **High**
Likely	🟩	🟧	🟥	🟥
Possible	🟩	🟧 **Medium**	🟧	🟥
Unlikely	🟩	🟩	🟧	🟥
Rare	🟩 **Low**	🟩	🟧	🟧

Appendix B
Definitions

Automated Decision System	A process, set of rules, or tool based on automated processing of data to perform calculations, create new data, or to undertake complex reasoning tasks. This includes advanced methods like artificial intelligence and machine learning, visual perception, speech or facial recognition, and automated translation between languages.
Data	Statistical, factual, quantitative, or qualitative information, in digital or analog form, that is regularly maintained or created by or on behalf of a City bureau and is in a form that can be transmitted or processed.
Data Governance	Definition of policies, processes and framework of accountability to appropriately manage data as a strategic asset.
Digital Age	This current era whereby social, economic and political activities are dependent on information and communication technologies. It is also known as the Information Age or the Digital Era.
Information	Information is the result of Data being processed, organized, structured or presented, allowing it to be used and understood.
Information Protection	A system of Data processing practices related to personally identifiable or identifying Data for the protection of privacy. This includes the management of individual pieces of personal Information, securing Data against unauthorized access, corruption or loss.
Metadata	A set of Data that describes and gives information about other Data, including its description, origination, and accuracy.
Open Data	Data that can be freely accessed, used, reused and redistributed by anyone.
Personal Information	Information about a natural person that is readily identifiable to that specific individual. “personal information,” which include, but are not limited to: • identifiers such as a real name, alias, postal address, unique personal identifier, online identifier IP address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers; • payment card industry such as bank account numbers or access codes; • personal health data, such as health history, symptoms of a disease, current health care information, medical device identifiers and serial numbers; • commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies; • biometric information; • internet or other electronic network activity information, that includes browsing history, search history, and information regarding a consumer’s interaction with an Internet Web site, application, or advertisement; • geolocation data, vehicle identifiers (including serial numbers and license plate numbers); • audio, electronic, visual, thermal, olfactory, or similar information; • professional or employment related information; • education information, provided that it is not publicly available; and • inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes
HRAR 11.04 Protection of Restricted and Confidential Information	

Privacy	The ability of an individual to be left alone, out of public view, and in control of information about oneself.
Confidential	Information that is made confidential or privileged by law or the disclosure of information that is otherwise prohibited by law or City policy.
Restricted	Some restrictions or limitations on the use of or disclosure of the information.
Principle of proportionality	The principle of proportionality requires that the processing of personal information must be relevant to, and must not exceed, the declared purpose
Surveillance Technologies	technologies that observe or analyze the movements, behavior, or actions of identifiable individuals in a manner that is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice.
Privacy terms	
Effectiveness	This refers to how a specific technology or solution fulfills the pursued objective.
Proportionality	Proportionality is a privacy principle that personal data collected and processed should be adequate, relevant, and limited to that necessary for purpose processed. Proportionality has multiple dimensions. Data collected and used should be adequate, because collecting too little information may lead to incorrect or incomplete information on a data subject. It should also be relevant and limited to what is necessary in relation to the purposes for which it is collected and processed ('data minimization'), both in terms of scope and time (data retention). The proportionality principles consideration of the amount of data to be collected. If excessive data is collected in relation to purposes, then it is disproportionate. Examples: Using biometric data like fingerprints to identify individuals when identity cards would suffice.
data protection	Data protection is the process of protecting data and involves the relationship between the collection and dissemination of data and technology, the public perception and expectation of privacy and the political and legal underpinnings surrounding that data. It aims to strike a balance between individual privacy rights while still allowing data to be used for business purposes. Data protection is also known as data privacy or information privacy. Data protection should always be applied to all forms of data, whether it be personal or enterprise. It deals with both the integrity of the data, protection from corruption or errors, and privacy of data, it being accessible to only those that have access privilege to it.
Frequency of the collection	Periodicity of the data collection.
Privacy safeguards	Measures designed to improve privacy and information protection. It can be represented as below, as, or greater than industry standard and best practices
privacy fundamental rights	Privacy fundamental rights are set to help individuals in being assured of the protection and privacy of their personal data. The General Data Protection Regulation contains a set of 8 privacy fundamental rights. These rights are not legally binding in the US.
Right to information	This right provides the individual with the ability to ask for information about what personal data is being processed and the rationale for such processing. For example, a customer may ask for the list of processors with whom personal data is shared.
Right to access	This right provides the individual with the ability to get access to personal data that is being processed. This request provides the right for individuals to see or view their own personal data, as well as to request copies of the personal data.

Right to rectification	This right provides the individual with the ability to ask for modifications to personal data in case the individual believes that it is not up to date or accurate.
Right to withdraw consent	This right provides the individual with the ability to withdraw a previously given consent for processing of personal data for a purpose. The request would then require stopping the processing of personal data that was based on the consent provided earlier.
Right to object	This right provides the individual with the ability to object to the processing of their personal data. Normally, this would be the same as the right to withdraw consent if consent was appropriately requested and no processing other than legitimate purposes is being conducted. However, a specific scenario would be when a customer asks that their personal data should not be processed for certain purposes while a legal dispute is ongoing in court.
Right to object to automated processing	This right provides the individual with the ability to object to a decision based on automated processing. Using this right, a customer may ask for this request (for instance, a loan request) to be reviewed manually, because of the believe that automated processing of the loan may not consider the unique situation of the customer.
Right to be forgotten	Also known as right to erasure, this right provides the individual with the ability to ask for the deletion of their data. This will generally apply to situations where a customer relationship has ended. It is important to note that this is not an absolute right and depends on your retention schedule and retention period in line with other applicable laws.
Right for data portability	This right provides the individual with the ability to ask for transfer of his or her personal data. As part of such request, the individual may ask for their personal data to be provided back or transferred to another controller. When doing so, the personal data must be provided or transferred in a machine-readable electronic format.

Privacy risk	The term “privacy risk” means potential adverse consequences to individuals and society arising from the processing of personal data, including, but not limited to: 1. Direct or indirect financial loss or economic harm; 2. Physical harm; 3. Psychological harm, including anxiety, embarrassment, fear, and other demonstrable mental trauma; 4. Significant inconvenience or expenditure of time; 5. Adverse outcomes or decisions with respect to an individual’s eligibility for rights, benefits or privileges in employment (including, but not limited to, hiring, firing, promotion, demotion, compensation), credit and insurance (including, but not limited to, denial of an application or obtaining less favorable terms), housing, education, professional certification, or the provision of health care and related services; 6. Stigmatization or reputational harm; 7. Disruption and intrusion from unwanted commercial communications or contacts; 8. Price discrimination; 9. Effects on an individual that are not reasonably foreseeable, contemplated by, or expected by the individual to whom the personal data relate, that are nevertheless reasonably foreseeable, contemplated by, or expected by the covered entity assessing privacy risk, that significantly: A. Alters that individual’s experiences; B. Limits that individual’s choices; C. Influences that individual’s responses; or D. Predetermines results; or 10. Other adverse consequences that affect an individual’s private life, including private family matters, actions and communications within an individual’s home or similar physical, online, or digital location, where an individual has a reasonable expectation that personal data will not be collected or used. 11. Other potential adverse consequences, consistent with the provisions of this section, as determined by the Commission and promulgated through a rule.
Risk of individual privacy harms	The likelihood that individuals will experience harm or problems resulting from personal data collection and processing
Risk of equity, disparate community impact	The likelihood that specific groups will experience harm or problems resulting from the collection of multiple sources of personal data and their processing.
Risk of political, reputation & image issues	The likelihood that collection or processing of private data may result in harm on professional or personal relationships, harm in reputation or image.
Risk of city business, quality & infrastructure issues	The likelihood that the collection or processing of private data may impact or expose city relationships, agreements, or any other contract, or the quality of those businesses, or built infrastructure
Risk of legal & regulatory issues	The likelihood of any violation of existing laws or regulations by the collection or processing of private information
Risk of financial Impact	The likelihood that ongoing costs in management, collection or processing of private data may become financially inviable or present costs that may not be considered