



# **BES Security LiveView (LVT) Mobile Security Observation Trailer Privacy Impact and Risk Analysis**

**Smart City PDX  
9-12-2022**



PRIVACY IMPACT AND RISK ANALYSIS REPORT [Template ver. 0.4]

1 of 18



This work is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/).



# PRIVACY ANALYSIS REPORT

City of Portland Privacy Toolkit

## WHAT IS THE PRIVACY 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 AN PRIVACY IMPACT ANALYSIS RECOMMENDED?

A PIA is recommended when:

- 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.

## HOW TO COMPLETE THIS DOCUMENT?

City staff complete two documents:

- *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: (1) Individual Privacy Harms; (2) Equity, Disparate Community Impact; (3) Political, Reputation & Image; (4) City Business, Quality & Infrastructure; (5) Legal & Regulatory; and, (6) Financial Impact. Then compares risks to the likelihood of happening to create a single risk measure based on the worst case scenario.

Risk Matrix	A: Low	B: Moderate	C: High	D: Extreme
Almost Certain	1A	1B	1C	1D
Likely	2A	2B	2C	2D
Possible	3A	3B	3C	3D
Unlikely	4A	4B	4C	4D
Rare	5A	5B	5C	5D





## Executive summary

The Bureau of Environmental Services is assessing the use of LiveView Mobile Security Observatory Trailer for BES facilities including remote pumping stations. When triggered, these mobile security platforms will provide live video feeds, illuminate the immediate area, and alert BES security – all during hours of darkness.

This assessment has found a **Medium** level risk in the worst case scenario. This means that the bureau needs to address some recommendations either to mitigate or manage risks.

This assessment highlights the following risks:


- The cameras will collect more information than is necessary to accomplish the purpose of the security cameras.
- Risks due to not relevant and necessary video footage, including individuals and children.
- Use of security cameras may restrict freedom of speech or association.
- Use of security cameras to monitor or surveil specific groups or people activity in the public realm.
- Storage of video for three years due to public records laws, if not litigated or involving criminal activity, increases the risk of unintended uses and impacts.

This assessment provide some details and recommendations on how to mitigate or manage the risks identified :

- Multiple types of collection devices bring different risks and management strategies. Optimize the field of view of the cameras to cover only the areas of interest and minimize any adjacent private property or the public realm.
- Minimize the collection of unnecessary footage, including individuals not involved in unlawful activities or children.
- Train City staff on identifying footage that is unnecessary, contain images that impact civil liberties of civil rights, or that could bring liability to the City. Work with City Attorneys and City privacy experts to request literacy and training materials.
- Inform local 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.
- 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. Reach out to the Public Records Office for more information about how to anonymize moving images. Recording audio conversation should be disabled.



# Privacy Impact Analysis

	Portland Privacy Analysis for a technology, project, data sharing agreement or app solution
<b>Information</b>	<b>Request information</b>
Bureau	Bureau of Environmental Services (BES)
Assessment done by	Hector Dominguez <a href="mailto:hector.dominguez@portlandoregon.gov">hector.dominguez@portlandoregon.gov</a>
Reviewed by	Judith Mowry - Office of Equity and Human Rights Eric Shaffner - City Attorney's Office
Date of Assessment	September 12, 2022
Document status	<b>Delivered to Bureau</b>
Name of the assessment	<b>BES Security LiveView (LVT) Mobile Security Observation Trailer</b>
General description	The Bureau of Environmental Services is assessing the use of LiveView Mobile Security Observatory Trailer for BES facilities including remote pumping stations. When triggered, these mobile security platforms will provide live video feeds, illuminate the immediate area, and alert BES security – all during hours of darkness.
<b>Evaluation topic</b>	<b>Assessment</b>
Purpose of the technology, project, data sharing or application	LiveView Technologies (LVT) provides surveillance technology using proprietary software and hardware for a 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 Service facilities like treatment plants and pumping stations. These trailers will not obstruct or interfere with pedestrian trails or public right of way.
Name of the entity owner of the application and website	LiveView Technologies. LiveView Technologies is a software company that provides security software and solutions. Based in Orem, Utah. <a href="https://www.lvt.com">https://www.lvt.com</a>
Type of Organization	Private entity





<p>Scope of personal data collected. List all sources of data and information.</p>	<p>Personal data collected from the CCTV surveillance cameras is contained in the footage livestreamed and recorded. Depending on the field of view of the cameras, footage can capture private property or public spaces where individuals, including images of children and people in vulnerable situations may also be captured. Full list of sensors are:</p> <ol style="list-style-type: none"> <li>1) 70-120° high resolution horizontal FOV (Field of View) Camera.</li> <li>2) PTZ (Pan-Tilt-Zoom) camera.</li> <li>3) 360° (panoramic) horizontal FOV (Field of View) camera.</li> <li>4) FLIR (Forward Looking Infrared) camera.</li> <li>5) two-way speaker</li> </ol> <p>The system has the capability of recording audio as well. Personal conversations may be unintentionally recorded.</p> <p>No additional automatic identification or tagging process is expected in this implementation; however, the vendor offers 'advanced security analytics' services.</p> <p>Product webpage: <a href="https://www.lvt.com/hardware/mobile-security-cameras">https://www.lvt.com/hardware/mobile-security-cameras</a></p>
<p>How personal data is collected</p>	<p>Only through video footage via the security cameras and additional sensors, including thermal images, infrared, and microphones, on the trailer. Some cameras collect images all the time, while some others may be triggered by a presence or motion sensor.</p>
<p>Who can access the data</p>	<p>The 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.</p> <p>The footage will be integrated to the Genetec security solution owned by BES</p>
<p>Purposes the data is used for</p>	<p>BES needs a security technology solution and LVT will support :</p> <ul style="list-style-type: none"> <li>- Security force and alerting multiplier</li> <li>- Meets operational continuity strategies</li> <li>- Deter theft and vandalism</li> <li>- Prevent thefts and other crimes at remote locations</li> <li>- Protect staff &amp; equipment</li> <li>- Uninterrupted service &amp; immediate notifications</li> <li>- Security bang for the buck</li> <li>- Self-sustaining mobile platform with no need to be supported or maintained by BES IT and/or BTS resources. LVT maintains the entire mobile platform.</li> <li>- Off-the-grid and low maintenance security equipment</li> <li>- Integrate with BES' Genetec security solution</li> </ul>
<p>Where the data is stored</p>	<p>Video footage and other sensor information is stored first in the units and sent to the vendors cloud servers. Footage can be downloaded by the customer and shared or processed independently.</p>
<p>How data is shared</p>	<p>Access to video footage is limited to those that need to manage the units at LVT and all access is logged.. footage and sensor data can be shared with law enforcement in cases of an incident or crime.</p>



<p>How long is the data stored?</p>	<p>The vendor stores video footage locally until it is pulled into our 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.</p> <p>In 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.</p> <p><a href="https://www.portland.gov/archives/retention-schedules">https://www.portland.gov/archives/retention-schedules</a>  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.</p> <p>Administrative ADM-0450  Retention schedule for Photographs, negatives, slides, digital, and moving images documenting City projects, activities, events, properties and responsibilities.</p> <p>Administrative - ADM-0570  Property Damage Records - If not litigated, retain 3 years after date of last action; if litigated, coordinate with the City Attorney's Office. It may contain confidential information.  <a href="https://oregon.public.law/rules/oar_166-200-0390">https://oregon.public.law/rules/oar_166-200-0390</a>  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.</p>
<p>Effectiveness</p>	<p>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.</p>





Proportionality, fundamental rights, frequency of the collection, and data protection and privacy issues line unintended data collection or processing.

CCTVs 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 bypassers or overviews of private property with no connection to any incident should be discarded immediately.

BES 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 and potentially criminal penalties if any misuse occurs in conformity with existing Human Resources rules, laws, and regulations.





<p>Privacy safeguards</p>	<p>In cases of public records requests, footage where people's faces will be blurred and anonymized</p> <p>Access to recorded footage, alerts, and real-time notifications will be constrained to the BES security team. The BES Security Manager will be responsible for these devices.</p> <p>Depending on the field of view of the cameras, footage can capture private property or public spaces where individuals, including images of children and people in vulnerable situations may also be captured. There are no clear measures for safeguard other than avoiding including private property zones in the camera field of view.</p>	
<p>Open source</p>	<p>No</p>	
<p>AI/ML claims</p>	<p>No</p>	
<p>Privacy Policy (link)</p>	<p><a href="https://www.lvt.com/legal">https://www.lvt.com/legal</a></p>	
<p>Privacy risk</p>	<p>Medium</p>	
<p>Surveillance Tech?</p>	<p>Yes</p>	
<td colspan="2" style="height: 30px;"></td>		
<p>Portland Privacy Principles (P3)</p>	<p><a href="https://www.smartcitypdx.com/privacy-principles">https://www.smartcitypdx.com/privacy-principles</a></p>	
<p>Data Utility</p>	<p>The collection of footage and sensor information stays on the device until an event or incident triggers an alert or notification.</p> <p>In addition to visual footage, the security trailer includes Optical, IR illumination, thermal, and fixed and pan-tilt-zoom (PTZ) configuration. Also a two-way speaker, which includes audio recordings. The potential of audio privacy risks is higher if the collection of audio recordings include private conversations.</p> <p>Not relevant footage and sensor data should be avoided to reduce privacy risks</p>	
<p>Full lifecycle stewardship</p>	<p>The full security data includes not only collected footage and sensor information, but also logs of incidents, alerts and notifications, and any note or comments from security personnel, transfers to third party vendors, like the Genetec Security Solution, and transfers to law enforcement agencies in case of criminal incidents and investigations.</p> <p>LVT, vendor and service provider, may have access to information stored in their devices on-site, but not share it to their customers or third parties. Footage stored on the vendor's cloud is only accessible to the customer, and the customer is responsible for maintaining, removing, or processing it.</p>	
<p>Transparency and accountability</p>	<p>It is very important to inform the neighbors, particularly those properties that may be within the field of view of the security cameras, about the purpose of the system and how to submit comments to the City.</p> <p>Another recommendation is to keep record of incidents and actions triggered by them. Compile those in an annual report that could be shared as open data.</p> <p>The BES Security Manager will be responsible for these devices. City employees could be subjected to administrative actions and potentially criminal penalties if any misuse</p>	







	occurs in conformity with existing Human Resources rules, laws, and regulations.
Ethical and non-discriminatory use of data	<p>Ethical issues may arise if specific groups are more impacted than others, particularly involving law enforcement. Becoming aware of what groups may be more involved and impacted with this security technology and work in prevention methods before correction may facilitate ethical and non-discriminatory actionable use of information.</p> <p>Working with different public safety groups may augment the information and intelligence around decision making. First responders like Portland Fire and Rescue and 911 calls (BOEC) may inform those decisions.</p>
Data openness	<p>Data openness helps to develop and nurture public trust. Keeping clear publicly available web pages with incident reports and equity analysis of the impacts can help with that.</p> <p>Informing neighbors, particularly those living closers and whose property, front yards, or moves going in and out their household could be capture by the security cameras field of view. Inform them about the measures to protect their privacy and potential benefits of the installation of these systems.</p> <p>Publish data about incidents in dashboards and make other public safety entities about this information. Exchange information responsibly, protecting personal identifiable information and anonymizing footage.</p>
Equitable data management	Try to collect demographic data from the incidents as much as possible and work with BES equity manager and other equity practitioners to identify impacts to specific groups and methods to prevent larger impacts.
Automated Decision Systems	<p>The footage and sensor information collected from the security trailer won't be part of any automated decision system.</p> <p>However, if image classification algorithms are involved, review this impact assessment.</p>
Optional	
Consent	Faces from individuals will be blurred. No other PII will be collected or used. Information involved in security incidents may be ruled under criminal and judiciary laws.



# Privacy Impact Risk Severity Assessment

WORST CASE SCENARIO	Medium
---------------------	--------

	Impact	Justification	Likelihood	Comments	Risk level
Individual Privacy Harms	Moderate	<p><b>1.1 The cameras will collect more information than is necessary to accomplish the purpose of the security cameras.</b></p> <p>This risk is connected to what the security cameras can access in their field of view and whether they have the ability to record activities happening in the public realm or private property. This could lead to unnecessary footage recording of private activities.</p> <p>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.</p> <p>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.</p> <p>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.</p>	Likely	<p>The following is an overview of the cameras used in the LVT security trailer system. All these cameras should follow the general mitigation recommendations in this assessment.</p> <p>1) 70-120° 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.</p> <p>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 BES 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 BES property. Inform the public about the practices using this type of cameras.</p> <p>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.</p> <p>4) FLIR (Forward Looking Infrared) cameras use thermographics images from the emission of infrared light.</p>	Medium





	Impact	Justification	Likelihood	Comments	Risk level
				<p>These cameras can be used to recognize a person from a critter or other animal, and any heat-emitting devices. These cameras have low privacy risks in general.</p> <p>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.</p>	





	Impact	Justification	Likelihood	Comments	Risk level
	Moderate	<p><b>1.2 Risks due to not relevant and necessary video footage, including individuals and children.</b></p> <p>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.</p> <p>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 the LVT security trailer are initially stored video on board and not not streamed up to the cloud until an incident has been detected.</p> <p>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 or not a real incident is or has happened.</p> <p>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 (<a href="#">ORS 30.831</a>).</p>	Likely	<p>These risks can be reduced by:</p> <ul style="list-style-type: none"> <li>a) Minimizing the access to video footage, particularly when no criminal activity or potential incidents are detected</li> <li>b) Provide proper training to operators on privacy protection and best practices in security under the Oregon Law.</li> <li>c) Reduce the retention time of non-relevant footage to a minimum.</li> <li>d) Train public records personnel to anonymize and blur a person's face in moving images.</li> </ul>	Medium





	Impact	Justification	Likelihood	Comments	Risk level
	High	<p><b>1.3 Recorded footage is accessed by unauthorized personnel</b> 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.</p>	Unlikely	<p>In order to mitigate individual privacy impacts the security team should:</p> <p>Follow cybersecurity and information protection best practices as described in the City's <a href="#">Information Security Administrative Rules</a>.</p> <p>Report any unauthorized access to the Information Security Office (<a href="#">BTS 2.08</a>)</p> <p>Periodically review access log files to the security system</p> <p>Minimize the collection of footage to the required when a security incident is in progress.</p> <p>Train operators and security personnel in incident and privacy breach response</p>	Medium
	High	<p><b>1.4 Personnel use cameras in unauthorized purposes</b> The risk that personnel use cameras for other purposes than protecting BES facilities and personnel may result in privacy breaches and impact organizational reputation.</p>	Unlikely	<p>Create a procedure to assess impacts of personnel using security equipment for other purposes.</p> <p>Train personnel about the responsibilities of using security equipment and impacts of unauthorized use of equipment.</p> <p>Create accountability measures that lead to corrective and remediation procedures. Follow existing Human Resources rules (<a href="#">HRAR-4.08 - Information Technologies</a>).</p> <p>Report these incidents as privacy breaches and include the action taken for remediation</p>	Medium





	Impact	Justification	Likelihood	Comments	Risk level
	High	<p><b>1.5 Recorded footage is shared to unauthorized third-parties</b></p> <p>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.</p>	Unlikely	<p>In order to minimize unauthorized sharing of information to third parties follow these recommendations:</p> <ul style="list-style-type: none"> <li>a) Ask personnel to request authorization before sharing to third parties.</li> <li>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.</li> <li>c) Train personnel on responsible data and information sharing practices.</li> <li>d) Work with City partners to create joint information protection practices to allow information sharing.</li> <li>e) Report any unauthorized information sharing.</li> </ul>	Medium
	Moderate	<p><b>1.6 Members of the public may not see the notice sign or may not be aware of why security cameras are necessary.</b></p> <p>Lack of public information about the implementation and use of surveillance and security equipment may lead 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.</p>	Possible	<p>The risk can be mitigated by the publication of information about this technology and its purpose, including this assessment. This public information needs to make clear that City properties are under surveillance and why the cameras are necessary.</p> <p>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 BES is protecting neighbors and individuals' privacy.</p>	Medium





	Impact	Justification	Likelihood	Comments	Risk level
	Moderate	<p><b>1.7 Risk of using live streaming features to monitor activities in the public realm or private property</b></p> <p>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.</p>	Unlikely	<p>In order to mitigate this risk:</p> <p>a) Limit the personnel with access to livestream video footage</p> <p>b) Implement periodic revisions of activity logs to identify unauthorized use</p> <p>c) Inform the public about the limitations and safeguards around live streaming video.</p> <p>d) Include information about the camera's field of view in privacy assessments</p>	Low
	High	<p><b>1.8 Risk of recording private audio conversations.</b></p> <p>The LVT security trailer includes a two-way speaker. The system has the ability to allow communication and record audio, potentially storing private conversation in the background not relevant to the operation of the security operations.</p>	Unlikely	<p>Oregon laws forbid to record private conversations with the proper consent from the parties [ORS 165.540 (1)(c)]</p> <p>To mitigate this risk constraint the use of audio systems is necessary to assure proper security operations.</p> <p>Do not record audio without the proper warrant.</p> <p>Immediately delete any unintentionally audio recording.</p> <p>Recording audio conversation should be disabled.</p>	Medium
Equity, Disparate Community Impact	High	<p><b>2.1 Use of security cameras may restrict freedom of speech or association.</b></p> <p>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 BES facility. Unless there is evidence of criminal activity that must be investigated or prosecuted, BES will not maintain those images for longer than the storage capacity. BES shares images only for legitimate law enforcement purposes or in response to public records requests.</p>	Unlikely	<p>To mitigate this risk,</p> <p>Train personnel involved in operating the cameras and managers in privacy protection practices, including civil liberties and civil rights</p> <p>Improve transparency measures by promptly releasing incident metrics and sharing of information, particularly during protests or civil disobedient events.</p> <p>Work with City Attorneys and privacy experts to request literacy and training materials.</p>	Medium
	High	<p><b>2.2 Use of security cameras to monitor or surveil</b></p>	Unlik	To mitigate this risk and impacts:	Medium





	Impact	Justification	Likelihood	Comments	Risk level
		<p><b>specific groups or people activity in the public realm.</b></p> <p>Besides protest and civil disobedience events around facilities, certain groups may feel specifically oversurveil or monitored, including people experiencing homelessness, and Black, Indigenous, and People of Color residents.</p>	ely	<p>Inform local 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).</p> <p>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.</p>	
<b>Political, Reputation &amp; Image</b>	High	<p><b>3.1 Risk of impacts on the City reputation and image.</b></p> <p>This risk may appear when a perceived failure in public trust appears. For instance, an information privacy breach or misused of equipment.</p>	Possible	<p>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.</p> <p>Transparency and accountability can be improved by informing the public about the purpose of the LVT security trailers and sensors on it. Information about what privacy safeguards are implemented, number of incidents and how they are resolved, and periodic reports can improve public trust.</p> <p>It is also recommended to reach out to local 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.</p>	Medium







	Impact	Justification	Likelihood	Comments	Risk level
City Business, Quality & Infrastructure	High	<p><b>4.1 Risk connected to mischaracterization or misidentification of contextual features in video footage</b></p> <p>This risk refers to the possibility of misidentifying an object or a context that may lead to a false positive incident detection.</p> <p>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.</p> <p>A City staff part of the BES 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 has to decide the thread level and the proper action.</p>	Unlikely	<p>Mitigation strategies include:</p> <p>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.</p> <p>b) Keeping proper equipment maintenance and working with the vendor to troubleshoot issues should reduce the likelihood for missing incidents.</p>	Medium
	High	<p><b>4.2 Incidents are not detected properly (false negatives)</b></p> <p>A false negative incident is when an activity that should have been detected is not. The LVT system has redundant systems; however lack of maintenance, low power, particularly in winter time, critters chewing on cables, vandalism, or the natural exposure to the environment may reduce equipment effectiveness.</p> <p>False negatives may end up with property damage, loss of goods in facilities, or even put personnel at risk.</p>	Unlikely	<p>Mitigation strategies include:</p> <p>a) Provide required maintenance to equipment and work with the vendor to troubleshoot issues with the equipment. Report any issue to the proper group.</p> <p>b) Training personnel to identify issues and resolve them may save time and increase effectiveness of the cameras.</p>	Medium





	Impact	Justification	Likelihood	Comments	Risk level
Legal & Regulatory	High	<p><b>5.1 Retention schedule is too long, increases the risk of unintended uses and impacts.</b> 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 (<a href="#">ORS 166-200-0405</a>).</p>	Possible	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
	High	<p><b>5.2 There is a risk of recording private conversations</b> The unintentional recording of people's voices and conversations outside the context of a criminal incident could be considered against the law. <a href="#">ORS 165.540 (1)(c)</a> forbids recording of audio conversations by any means.</p>	Unlikely	FOIA requests or sharing to third parties, including law enforcement, may be against the Oregon Law. 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.	Medium
	High	<p><b>5.3 Video footage is not properly anonymized</b> Blurring faces and properly anonymizing individuals 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.</p>	Possible	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. 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.	Medium
Financial Impact	High	<p><b>6.1 Risks of property loss or damage due to faulty equipment</b> 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.</p>	Unlikely	<p>Mitigation strategies include:</p> <ul style="list-style-type: none"> <li>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.</li> <li>b) Periodically assess if the equipment is at risk.</li> <li>c) Provide training to security personnel on how to respond to attacks to critical infrastructure or equipment</li> </ul>	Medium

