Small Unmanned Aerial System (sUAS) Pilot Project

Privacy Impact Assessment

Delivered

Smart City PDX

July 21, 2022

PRIVACY IMPACT ASSESSMENT REPORT

City of Portland Privacy Toolkit

WHAT IS THE PRIVACY IMPACT ASSESSMENT?

The Privacy Impact Assessments ("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 impacts and risks and lead to proper strategies for risk mitigation or alternatives that may even remove those identified risks.

The Privacy Impact Assessment may lead to a more comprehensive 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 THRESHOLD PRIVACY 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 Threshold 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. This report is a summary of the analysis.
- *The Comprehensive 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.

Executive summary

Portland Police Bureau (PPB) is planning a pilot program using Small Unmanned Aerial Systems (sUAS), also commonly referred to as “Drones”. sUASs are widely used in the public sector, including nearly every jurisdiction within the Portland Metro area. The regulated use of sUASs by the PPB Investigations Branch will provide improvements in safety for both officers and community members. Additionally, the use of sUAS technology in crime / major crash scene events reduces inconvenience to the public by significantly reducing documentation time at a scene.

The privacy Impact Assessment shows a **Medium Risk** worst case scenario.

UAS are usually perceived as a major privacy concern due to the collection of video footage over people and people’s properties. However, this pilot program constraints the use of UAS and how collected information is used, shared, processed, and deleted.

Main privacy risks and impacts include:

1. Risk and impacts on Civil Rights and Civil Liberties
2. Unauthorized data sharing
3. Risk of privacy data breach
4. Risks due to lack of transparency
5. Risks due to lack of oversight and public reporting

This report describes these risks and other identified issues. Some of the main recommendations to mitigate these risks include:

1. Specific trainings to staff and operators on civil liberties and civil rights
2. Include privacy impact assessments of sensors mounted on UAS and vendors
3. Identify no-fly zones and high sensitive areas like churches, temples, schools, hospitals and prepare scenarios where UAS needs to fly over these zones.
4. Collect demographic anonymized information involved in cases for equity assessments
5. Work on information protection best practices to minimize the risk of a privacy breach.
6. Work with the City’s Information Security Office to minimize cybersecurity threads.
7. Proactively inform about operations as much as the law allows. Include periodic reports to the City Council.

Threshold Privacy Analysis

	Portland threshold privacy analysis for a technology, project, data sharing agreement or app solution
Version 0.3	**This information is considered restricted and for internal use only until the client clears it to the public. This notice must be remove when authorized for publication**
Information	**Request information**
Bureau	Portland Police Bureau
Client	Art Nakamura
e-mail	Art.Nakamura@portlandoregon.gov
Assessment done by (name/email)	Hector Dominguez / hector.dominguez@portlandoregon.gov
Date of Assessment	July 14, 2022
Document status	**Restricted**
Date of Acceptance	**(Add Date)**
Authorized by	**(Add Name and Signature)**
Name of the assessment	**Small Unmanned Aerial System (sUAS) Pilot Project**
General description	sUAS is the term used for Small Unmanned Aerial Systems, also commonly referred to as “Drones”. sUASs are widely used in the public sector, including nearly every jurisdiction within the Portland Metro area. The regulated use of sUASs by the PPB Investigations Branch will provide improvements in safety for both officers and community members. Additionally, the use of sUAS technology in crime / major crash scene events reduces inconvenience to the public by significantly reducing documentation time at a scene. PPB sUASs are exact or slightly modified versions of commercially available products and will be clearly marked with City of Portland or Portland Police logo.
Evaluation topic	**Assessment**
Purpose of the technology, project, data sharing or application	The regulated use of sUASs by the PPB Investigations Branch will provide improvements in safety for both officers and community members. Additionally, the use of sUAS (Unmanned Aerial System) technology in crime / major crash scene events reduces inconvenience to the public by significantly reducing documentation time at a scene.

Name of the entity owner of the application and website	Internal pilot project from Portland Police Bureau's Major Crash Team (MCT) and the Explosive Disposal Unit (EDU)
Type of Organization	Government
Scope of personal data collected. List all sources of data and information.	Scope of data collection TRAFFIC DIVISION • Document scenes of Major Crash Team activations • Document post-crash vehicle damage • Conduct traffic flow / pattern studies of high crash roadways • Provide sUAS support during Search and Rescue Operations EXPLOSIVE DISPOSAL UNIT • Quickly gather information on suspicious items from a distance • Search immediate area for secondary devices • Visually clear potential blast area of community members • Confirm location of items following render safe operations • Provide sUAS support during tactical events upon request of Critical Incident Commander (CIC) • Provide immediate support during disasters, building collapse, ie. Safeway Roof Collapse Sources of data come from sensors mounted on the UAS. The pilot program will use Forward Looking Infrared Real-Time Video (FLIR) cameras. FLIR cameras present an image that could be de-identified. Additional sensors may add privacy risks and impacts.
How personal data is collected	Personal information gets collected through police forms connected to the specific case where the UAS is used. sensors mounted on UAS may acquire contextual information that could also identify individuals. Disclosure of sensitive information like the presence of children, victims, and imagery representing crime scenes may impact individuals or groups. Common uses of camera mounted on drones include: (1) Regular still images (2) Regular video images (3) Thermal still and video images (4) 3D video images and LIDAR sensors (5) Radar
Who can access the data	Portland Police Bureau Traffic Division and the explosive disposal unit only in operations authorized by the scope of the UAS pilot. The Portland Police Bureau Air Support Unit (ASU) is a regional team that provides aerial support and expertise for the City of Portland's investigative and administrative needs. The goal of the Air Support Unit is to enhance the safety

	of the community and police personnel through the strategic deployment of airborne technologies.
Purposes the data is used for	Only for field assistance and support during tactical events, investigative, training, and administrative needs.
Where the data is stored	Portland Police Bureau's Investigations branch will store data and information according to the Criminal Information System
How data is shared	Data won't be shared outside the stakeholders involved in this pilot program
How long is the data stored?	All video recordings and photos will be retained in accordance with public records law, PPB policy, the PPB UAS program retention schedule and ORS 837.362 Policies and Procedures for Use of Data resulting from the use of UAS.
Effectiveness	As much as the use of UAS is constrained to tactical cases and authorized investigative purposes where there is no viable alternative to the use of UAS and sensors attached to it.
Proportionality, fundamental rights, frequency of the collection, and data protection and privacy issues line unintended data collection or processing.	Use of UAS camera systems will be conducted in a professional, ethical and legal manner. Camera systems lawfully deployed without a search warrant, or valid warrant exception, will not invade the privacy of individuals, or look into areas where a reasonable expectation of privacy exists. Operators will avoid recording or transmitting images of any location where a person would have a reasonable expectation of privacy. Pilot stakeholders will adhere to all laws governing the use of airborne cameras and thermal imaging systems for searches. When a search utilizing a thermal imaging system or UAS' camera system is conducted under the authority of a search warrant, a copy of the warrant will be included with the post flight crew report. Video recordings and photos will only be taken in situations where there is a reasonable expectation that the data will contain evidentiary value and in situations where it will provide public transparency of flight operations. Video recordings and photos may be taken for training purposes when precautions have been taken to avoid collecting any personally identifiable information of any person with a reasonable expectation of privacy.
Privacy safeguards	Portland Police Bureau follows the Criminal Justice Information System standard. Collected information will not be shared outside the stakeholders of the UAS pilot.
Open source	No
AI/ML claims	No
Privacy Policy (link)	https://www.portland.gov/help/about/privacy
Privacy risk	Medium
Surveillance Tech?	Yes

Portland Privacy Principles (P3)	
Data Utility	Data collected by PPB units is minimized and used only to provide contextual and environmental information in major crime or major crash scene events
Full lifecycle stewardship	The privacy impact assessment is limited to the UAS and its Standard Operating Procedures do not include the sensors necessarily. End of life of equipment and deletion of materials collected after a flight is not defined in the Standard Operating Procedures.
Transparency and accountability	PPB is documenting each the RPIC Flight with a Report that includes the following fields: • Date • Time • Location • Purpose of flight • Supervisor approving flight • Crew members assigned • Duration of flight • Disposition of digital media evidence and other data gathered • Summary of activities • Outcome of deployment • Supervisor Approving the Post Flight Report This report does not include the type of cameras and sensor onboard. Each flight will also include a logbook with the following fields: • Date • Time • Location • Crew members assigned • Flight duration • Any repairs completed or equipment/performance discrepancies noted Audits on the documentation will be done monthly by the ASU sergeant, and documented. A Memorandum will be forwarded through the chain of command to the branch assistant chief. It is not clear if these documents will be made available publicly.

Ethical and non-discriminatory use of data	Forbidden use of the UAS equipment: Conduct random or indiscriminate mass surveillance activities. Target a person based solely on individual characteristics, such as, but not limited to race, ethnicity, national origin, religion, disability, economic source or status, housing status, gender or sexual orientation. Harass, intimidate or discriminate against any individual or group. Conduct personal business of any type. Crowd control / crowd management, unless a life safety critical incident occurs. To be weaponized (ORS 837.365). Be used in conjunction with any type of facial recognition technology
Data openness	The Standard Operating Procedure does not describe whether documentation or reporting will be made open or publicly accessible. Also, it does not include a step for creating an annual usage report to City Council
Equitable data management	No considerations for equitable data management in cases that incidents may over represent certain groups.
Automated Decision Systems	The UAS won't include any automated decision system
Optional	
Consent	The collection of data will be in response to major crime or crash events. No consent is asked in those cases and the data will be subjected to judiciary law regulations. However, there is a case where a UAS could be used with written consent of an individual for the purpose of acquiring information about the individual or the individual's property (ORS 837.330).

Privacy Impact Risk Severity Assessment

WORST CASE SCENARIO	Medium

Severity (Evaluate for the worst / highest possible impact)					
Risk Type	**Impact**	**Justification**	**Likelihood**	**Comments**	**Risk level**
Individual Privacy Harms	High	1.1 Risk of Individual civil liberties and civil rights violations due to: Collection of data and personal information coming from individuals, including those engaging in constitutionally protected activities, even if they have not been accused of a crime. Use of UAS surveillance on protestors Unwarranted searches to private property	Possible	- Assure that employees and contractors complete privacy awareness, civil rights and civil liberties, ethics, code of conduct. and any other related training. - Create mechanisms that assure UAS are restricted to the specified applications in the SOP. - Create a process for remediation in cases of impacts in civil liberties and Civil Rights. - Work with Civil liberties and Civil Rights organizations and advocacy groups, informing them about the policies and specific uses of UAS. - Minimize retention time of information not connected to any investigation to 24 hours max. - Perform independent privacy impact assessments for individual sensors (visual, FLIR, Radar, etc) and publish the analysis and actions to mitigate risks and impacts just for the sensors and specific vendors. - Identify no-fly or highly sensitive zones, potentially working with community and local organizations to inform and define such zones. These sensitive zones could include schools, hospitals, and churches and spaces for worship.	Medium

Severity (Evaluate for the worst / highest possible impact)					
Risk Type	**Impact**	**Justification**	**Likelihood**	**Comments**	**Risk level**
	High	1.2 Additional risks due to third-party unauthorized data sharing. If data gets shared to: - with other groups within the agency - with other agencies - with other jurisdictions - With apps and service providers - with service providers third-parties	Unlikely	- Train staff on what the policies for data sharing to third parties are. Perform regular audits on data. - Develop data governance policies for data collected or derived from the use of UAS - Use data encryption as allow by law	Medium

Severity (Evaluate for the worst / highest possible impact)					
Risk Type	**Impact**	**Justification**	**Likelihood**	**Comments**	**Risk level**
	Moderate	1.3 Risks due to capturing the identity or recording the activity of persons.	Unlikely	The Standard Operating Procedure contains already measures to protect individual privacy. To further assuage public concerns about identity capturing and/or activity monitoring. - Do not capture still or video footage of persons in areas where there is an expectation of privacy without the individual's permission, unless responding to an emergency as described in the pilot. - As much as possible, provide advance and ongoing notice that a UAS will be or it is in operation. - Where PII, such as faces, license plates, and house numbers, is captured in camera or video footage that is retained by PPB that data will be obfuscated through technical means, such as blurring, pixilation, blocking, or redaction of hard copies, such that it is no longer identifiable or reasonably re-identifiable.	Low

	Moderate	1.4 Risk of not providing reasonable expectation of privacy	Unlikely	Some specific areas may have additional expectations of privacy. Assess if any specific privacy strategy is needed for these spaces. Areas that may have a reasonable expectation of privacy may include, but not limited to: 1. Commercial facilities (operated by private entities): a. Factories b. Warehouses c. Office buildings d. Hotel rooms, except for lobbies or corridors e. Other buildings in which employment may occur. 2. Private clubs and religious organizations a. Churches, synagogues, mosques b. Private clubs where members must pay dues. 3. Private homes/residences a. Any home, condominium or apartment that is used exclusively as a private residence, except in common areas like a lobby. 4. Protected areas in jailhouses, or in property owned by other jurisdictions. 5. Vehicles - Train personnel on privacy strategies that could include: post anonymization and de-identification of individuals, protection of minors, identify sensitive information that can include medical conditions, financial data, biometric information, or contextual information that can increase the risk for re-identification or create individual, collective, property, or any other material harm.	Low

Severity (Evaluate for the worst / highest possible impact)					
Risk Type	**Impact**	**Justification**	**Likelihood**	**Comments**	**Risk level**
Equity, Disparate Community Impact	High	2.1 Risk of over use of UAS on specific groups or neighborhoods	Unlikely	- Collect demographic anonymized information of individuals involved in the use of UAS. - Report analysis of demographic data and release it in public forums and in the form of open data. - Perform equity and data justice analysis of demographic data.	**Medium**
	Moderate	2.2 Methods of reporting disproportionately impact specific groups or neighborhoods	Unlikely	Use equity analysis and data justice frameworks to publish information, particularly demographic data. If releasing information impacts a specific group disproportionately, create spaces for discussing these results with local organizations and members of the impacted community. - Assign resources to provide equity and data justice analysis to data collected and derivative reports. - Use accessible language to publish reports and dashboards.	**Low**

Severity (Evaluate for the worst / highest possible impact)					
Risk Type	**Impact**	**Justification**	**Likelihood**	**Comments**	**Risk level**
Political, Reputation & Image	High	3.1 Risk of a privacy data breach or data related issue	Possible	To assuage potential privacy and civil liberties arising from uncertainties regarding UAS data access, use, storage, security, and the accountability of handlers and owners of that data, the following mitigating steps are recommended: - Collect information using UAS, or use UAS-collected information, only to the extent that such collection or use is consistent with and relevant to an authorized purpose. - PII collected with UAS that cannot be technically obfuscated needs to be used solely for the authorized purpose. - Minimize the retention of any PII that does not serve the authorized purpose. - Constraint the sharing of video or any other footage collected by the UAS to the specified authorized purpose defined in the SOP. Any sharing of information to any law enforcement agency or system should be done under the law and existing regulations. - Make the usage report available to the public and reviewed and approved by Portland City Council.	Medium
	Moderate	3.2 Lack of trust due to third parties not authorized to be used.	Possible	Certify third party users and minimize external processing of data to avoid any misuse or potential of data privacy breach.	Medium

Severity (Evaluate for the worst / highest possible impact)					
Risk Type	**Impact**	**Justification**	**Likelihood**	**Comments**	**Risk level**
	High	3.3 Lack of transparency	Possible	Lack of transparency usually translates into a reduction of public trust and allowing misinformation streams to create narratives that damage public image. Transparency can be increased by: - Informing the public about ongoing operations and reporting after incidents - Allow visual Identification of equipment and teams while in operation - Allow digital identification in the form of Remote identifiers while in operation of equipment (https://www.faa.gov/uas/getting_started/remote_id/drone_pilots) - Report and allow access to public documentation of flights and operations - Proactively share data, reports and information about the cases according to the law	Medium

Severity (Evaluate for the worst / highest possible impact)					
Risk Type	**Impact**	**Justification**	**Likelihood**	**Comments**	**Risk level**
	High	3.4 Lack of oversight and credible audits	Possible	- Develop processes for internal audits and release them publicly. - Include reputable and neutral third party audits and release results. - Develop processes and data systems that facilitate audits. - Release reports of use and performance of UAS to the City Council. - Connect with Police advisory and technology oversight groups and share UAS usage reports with these groups.	Medium
City Business, Quality & Infrastructure	High	4.1 Risk from lack of internal data protection	Unlikely	- Work with the City's information security office to assure that information protection systems are in place. Release cybersecurity audits and reports according to the accepted risks and law.	Medium

Severity (Evaluate for the worst / highest possible impact)					
Risk Type	**Impact**	**Justification**	**Likelihood**	**Comments**	**Risk level**
	High	4.2 Risk of privacy breach (external to the City)	Unlikely	Privacy breaches can have different sources, including: - Operators or Pilots in Command (PIC) - Visual observers - Storaged data after the event. Some recommendations to reduce this risk are: - Develop equipment procedures that support operators and PIC access to information securely. - Make sure visual observers are out of range and to a secure distance from operators and PIC. - Make sure equipment and all radio transmissions are also protected, encrypted, and with robust cybersecurity measures. - Include cybersecurity measures to personnel access and other authorized use of information after the incident. - Include proper procedures to destroy data for end-of-life of equipment and after regular operations, including inflight memories, removable card memories, and other temporary data storage units.	Medium

Severity (Evaluate for the worst / highest possible impact)					
Risk Type	**Impact**	**Justification**	**Likelihood**	**Comments**	**Risk level**
	Moderate	4.3 Risk of lower quality of service due to lack of training	Unlikely	Assuring Quality of Service (QoS) of operators and Pilots in Command (PIC) depends on the training and certifications needed for specific functions, including equipment maintenance. Given that the Standard Operating Procedures include training, this risk is set as unlikely; however, wrong readings, interpretation, and errors in operation may greatly impact the use and results of UAS.	Low

	Moderate	4.4 Risk of low quality of service (QoS) of equipment and other measurement errors	Possible	Given that the use of UAS includes commercial and off-the-shelf equipment, it is important to set minimum equipment requirements and work with manufacturers if needed. This risk should also include sensors attached to it. Given that commercial off-the-shelf equipment will be used, PPB needs to make sure that data are properly secured, stored, and disseminated include: - encrypting the transmission of UAS video; - restricting access to real-time video to authorized users with a need to know; - restricting disclosure of analytical products that contain UAS-obtained images to approved requesters and redacting law enforcement sensitive, personally identifying information, and other sensitive information prior to disclosure, unless the requester has a need to know; - maintaining a log to track the dissemination of all analytical products that contain UAS-obtained images; and handling UAS-obtained images that are to be used as evidence in accordance with rules of evidence, such as ensuring they are not co-mingled with information from other investigations and maintaining an adequate chain of custody. - Regarding sensors QoS verify performance measures like resolution, rates of data acquisition, encryption methods, operating condition (for instance, temperature range of operations, acceleration range and impact forces) - Additional QoS verification can include energy consumption, batteries and energy storage, radio communication security and range, geolocation accuracy, and other maneuverability parameters.	Medium

Severity (Evaluate for the worst / highest possible impact)					
Risk Type	**Impact**	**Justification**	**Likelihood**	**Comments**	**Risk level**
Legal & Regulatory	High	5.1 Risk of misuse, abuse, or use outside the SOP	Unlikely	Use outside the specified tasks in the Standard Operating Procedures may impact public trust and could even be illegal depending on the context. Develop proper training and employee and operator awareness of the approved uses. This training is included in the SOP, therefore this risk is unlikely. - Include preventive and corrective measures of misused equipment. - Report misuse or abuse of equipment or access to information promptly to City authorities.- Work with equity and human rights personnel to assess whether any equitable or civil rights impacts were involved in the misuse of the equipment - Assess impacts of the misuse or abuse of equipment and assign a team to work on remediation strategies.	**Medium**
	Moderate	5.2 Risk of not conforming with Oregon Law	Unlikely	Oregon law ORS 837 (https://oregon.public.law/statutes/ors_chapter_837) describes the legal operation of an Aircraft. The Standard Operating Procedures align to Oregon Law and this risk is unlikely. In order to assure compliance with the law it is recommended to have both Internal and external audits that can be publicly accessible.	**Low**

Severity (Evaluate for the worst / highest possible impact)					
Risk Type	**Impact**	**Justification**	**Likelihood**	**Comments**	**Risk level**
	High	5.3 Risk from the requirement from FAA to have UAS registered and requesting a certificate waiver or authorization: https://www.faa.gov/uas/public_safety_gov/public_safety_toolkit	Unlikely	Having unauthorized UAS used by the City may impact the program and its reputation. It is an unlikely scenario, but the FAA regulations of flying UAS in urban areas are constantly changing and being upgraded. It is important to keep the program and operators informed about FAA rules and assure that operators have the proper certifications for flying and using the equipment.	Medium

	High	5.4 Risks coming from FAA UAS operation rules like: FAA has publishes a playbook for public safety drone operations: https://www.faa.gov/sites/faa.gov/files/uas/public_safety_gov/public_safety_toolkit/Public_Safety_Drone_Playbook.pdf	Unlikely	The FAA includes a set of public safety operations of UAS. The Standard Operating Procedure (SOP) does not include them explicitly; however, the risks described by the FAA are unlikely. The recommendation is to add them to the SOP and create a mitigation strategy for these safety risks: - Define a minimum operating altitude to the ground for safe operation in compliance with FAA regulations. - Define response in immediate emergency situations include those caused by equipment malfunction or weather conditions - Report incident to FAA for each instance it flies outside the FAA Certificates of Authorization (COA)-designated or restricted airspace without permission Make sure that the following situations are addressed: - Operating from a moving vehicle (may be allowed in certain instances, but the FAA investigation can make that determination) - Operation of multiple unmanned aircraft by the same individual - Carriage of hazardous material - Operation over human beings (most likely, crowds of people; estimate/use descriptors to illustrate crowd density) - Temporary Flight Restriction (TFR) violations - Object dropped from the drone	Medium

Severity (Evaluate for the worst / highest possible impact)					
Risk Type	**Impact**	**Justification**	**Likelihood**	**Comments**	**Risk level**
	High	5.5 Risk due to non-standard UAS operations like: - Operating low over the heads of non-participating persons (notably if individuals moved out of the way to avoid the drone) - Flying between vehicles or operating over a roadway in use - Chasing people or pets - Attaching a firearm or weapon to the drone - Injuries to people or damage to property	Unlikely	The FAA also includes non-standard UAS operation conditions. The recommendation is to include in the Standard Operating Procedure and operators training those non-standard cases. Make sure that all these non-standard operating cases are in compliance with ORS 837 and any other applicable law and regulation.	Medium
Financial Impact	Moderate	6.1 Risks of accidents, damage to public property, City property loss, staff injuries, public injuries.	Unlikely	The City should have an insurance policy regarding compensation in cases of property damage. Make sure operators, maintenance personnel, and Pilots in Command (PIC) are trained to minimize property damage, including the equipment and sensors themselves.	Low
	Moderate	6.2 Risks of fines for not compliance to FAA regulations or Oregon Law.	Unlikely	This is a low risk scenario. Make sure that certification and audits and documentation are up to date.	Low

Severity (Evaluate for the worst / highest possible impact)					
Risk Type	**Impact**	**Justification**	**Likelihood**	**Comments**	**Risk level**
	High	6.3 Risks of lawsuits and other liability due to misuse of UAS	Possible	Operating a UAS makes the City liable to lawsuits. Document flights and operations in a way that allows proper oversight and improves operations. Work with City Attorneys to prepare cases when a lawsuit happens.	Medium
	Moderate	6.4 Risks of compensation due to damages from privacy breaches.	Possible	The regulation in Oregon on compensation for damages created due to data breaches is not completely clear. The process usually goes to courts. Avoiding a data breach is the first step, but in the rare event of a privacy data breach, work with City Attorneys to comply with the law.	Medium