Portland Police Bureau Unmanned Aerial System (UAS) Program

Privacy Impact Assessment

Final and released version.

Smart City PDX

May 31, 2024

PRIVACY IMPACT ASSESSMENT REPORT

City of Portland Privacy Toolkit

WHAT IS THE PRIVACY IMPACT ASSESSMENT?

The Privacy Impact Assessment ("PIA") is a method to quickly evaluate 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 interest 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 A 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 Privacy Analysis.* 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 Risk Types 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. It then compares those risks to their likelihood of occurring to create a single risk measure based on the worst-case scenario.

Executive summary

This Privacy Impact Assessment of the Portland Police Bureau's (PPB) use of Unmanned Aircraft Systems (UAS), also commonly referred to as drones, is a revision of PPB's 2023 sUAS Standard Operating Procedure (SOP), was prompted by an update to the SOP that extends and consolidates the use of UAS by PPB.

This PIA concludes, in part, that there has been a consistent reduction of risks by PPB since the issuance of the first PIA thanks to improvements in best practices, public information, the Standard Operating Procedure policy, and in diligently reporting deployments.

UAS are usually perceived as a major privacy concern due to the collection of video footage over people and people's properties. 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

Summary of main changes in the new SOP:

- PPB has a new host program: the Specialized Resources Division (SRD). SRD responsibilities include Air Support Unit, Crisis Negotiation Team, Explosive Disposal Unit, Special Emergency Reaction Team, Canine Unit, Narcotics and Organized Crime Unit, and the Traffic investigations Unit (TIU).
- In addition, other teams can access sUAS:
    - Behavioral Health Unit (BHU).
    - Metro Explosive Disposal Unit (MEDU)
- The main authority for the use of UAS is the SRD commander.
- Deployment is only authorized to trained members of SRD.

The new SOP authorizes use of UAS for:

- Enhancing protection of lives and property when other means and resources are not available or are less effective or existing tactics need to be augmented.
- Uses under conditions authorized by State law:
    a) Pursuant to a valid warrant authorizing its use (ORS 837.320(a)).
    b) When there is "probable cause to believe that a person has committed a crime, is committing a crime or is about to commit a crime, and exigent circumstances exist that make it unreasonable to obtain a warrant authorizing [its] use . . ." (ORS 837.320(b)).
    c) With written consent of an individual for the purpose of acquiring information about the individual or the individual's property (ORS 837.330).
    d) As part of search and rescue activities (ORS 837.335(1)).

e) For assisting an individual in an emergency where there is a reasonable belief "that there is an imminent threat to the life or safety of the individual . . ." (ORS 837.335(2)(a)).
f) During a state of emergency declared by the Governor (ORS 837.335(3)), if:
    1. The UAS is used only for "preserving public safety, protecting property or conducting surveillance for the assessment and evaluation of environmental or weather-related damage, erosion or contamination . . ."
    2. The UAS operates "only in the geographical area specified in [the Governor's] proclamation . . ."
g) For "reconstruction of a specific crime scene or accident scene, or similar physical assessment, related to a specific investigation" (ORS 837.340).
h) For training in the use and acquisition of information (ORS 837.345).

The SOP includes reasonable privacy measures like forbidding intentionally recording or transmitting images of any location where a person would have a reasonable expectation of privacy (e.g., residence, yard, enclosure) and avoiding inadvertently recording or transmitting images of areas where there is a reasonable expectation of privacy. Reasonable precautions include deactivating or turning imaging devices away from such areas or persons during operations.

The use of sensors like thermal imaging systems or regular vision cameras for searches requires a search warrant. Video recordings will be taken only if it would be reasonable to expect that the resulting data will contain evidentiary value, if the recordings will provide public transparency of flight operations, or if they will assist in training.

UASs are widely used in the public sector, including nearly every jurisdiction within the Portland Metro area. PPB has developed a publicly accessible UAS flight and operations open data dashboard. Information can be downloaded as a CSV file.

The privacy Impact Assessment shows a **Medium Risk** worst case scenario. The main recommendations of this assessment include:

1. Provide specific training to staff and operators on identifying privacy issues and balancing the use of UAS and sensors mounted on them and techniques and strategies to protect people's privacy.
2. Keep the existing public dashboard[1] updated with latest flight logs and information. Include detailed information for high public interest cases.
3. Create a process for remediation and public input in cases of impacts to civil liberties and civil rights due to privacy issues.
4. Include third-party and neutral information audits to ensure public trust and effectiveness of internal audits and supervision.
5. Keep an open channel for public input and communications.

[1] https://www.portland.gov/police/community/drones

6. Identify additional no-fly zones and highly sensitive areas like churches, temples, schools, and hospitals and prepare for scenarios where UAS needs to fly over these zones.
7. Work with the City's Information Security Office to minimize cybersecurity threats and attacks on UAS.
8. Proactively inform the public about operations to the extent allowed by law. Include meaningful metrics and public engagement in the annual public report.

Privacy Analysis

Purpose of the technology, project, data sharing or application

UAS is the term used for Unmanned Aircraft Systems, also commonly referred to as drones. UASs are widely used in the public sector, including nearly every jurisdiction within the Portland Metro area. The regulated use of UASs by the PPB Investigations Branch will provide improvements in safety for both officers and community members. Additionally, the use of UAS technology in crime / major crash scene events reduces inconvenience to the public by significantly reducing documentation time at a scene.

PPB UASs are exact or slightly modified versions of commercially available products and will be clearly marked with City of Portland or Portland Police logo.

Name of the entity owner of the application and website

Portland Police Bureau
https://www.portland.gov/police/community/drones

Type of Organization

Government

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

The information collected by UAS can be used to gather intelligence and contextual information during an ongoing case, use as evidence, and other assistive purposes as defined in the authorized uses below.

Authorized uses of UAS are:

a. Pursuant to a valid warrant authorizing its use.
b. When there is probable cause to believe that a person has committed a crime, is committing a crime, or about to commit a crime, and exigent circumstances exist that make it unreasonable to obtain a warrant authorizing its use.
c. With written consent of an individual for the purpose of acquiring information about the individual or the individual's property.
d. As part of search and rescue activities.
e. To assist an individual in an emergency where there is a reasonable belief there is an imminent threat to the life or safety of the individual.
f. During a state of emergency declared by the Governor, if:
    i. The UAS is used for preserving public safety, protecting property, or conducting surveillance that will be used to assess and evaluate environmental or weather-related damage, erosion, or contamination.
    ii. The UAS operates in the geographical area specified in the Governor's

proclamation.

g. To reconstruct a specific crime scene, or accident scene, or a similar physical assessment, related to a specific investigation.
h. For training in the use and acquisition of information.

Sources of data come from sensors mounted on the UAS. The use of sensors includes 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

Video resolution is set at 720 dpi by default.

Who can access the data?

The Portland Police Bureau's Specialized Resources Division (SRD), the Traffic Investigations Unit (TIU), the Metro Explosive Disposal Unit (MEDU), and the Air Support Unit (ASU). All Remote Pilots in Command approved by the SRD Commander and members trained and authorized by SRD are the only ones to deploy a UAS.

Information gathered by UAS can be accessed by other internal groups at Portland Police Bureau.

Purposes the data is used for.

Only for field assistance and support during tactical events, investigative, training, and administrative needs.

The Specialized Resources Division (SRD).
Gather information to enhance the protection of lives and property when other means and resources are not available, are less effective, or as a tool to augment existing tactics.

The Traffic Investigations Unit (TIU) will include collecting information for:
• 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

The Metro Explosive Disposal Unit (MEDU):
• 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, e.g., Safeway Roof Collapse

The Air Support Unit (ASU):
Information to oversee compliance with FAA regulations and applicable laws.
Required information to generate reports to the FAA and Oregon Department of Aviation.
The Specialized Resources Division Commander or designee may independently audit or gather information on any UAS deployment to ensure its validity and adherence to all rules and regulations.

Where the data is stored

Portland Police Bureau's Investigations branch will store data and information according to the Criminal Information System. The information is managed by the Police Bureau DIMS system, which is the photo and video storage system for all police bureau video/photographic evidence.

How data is shared

Information will be shared as evidence for investigations into authorized groups and under existing police records regulations. Access log files are shared to regularly schedule audits. The information system includes an automatic audit trail.

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 Oregon's Policies and Procedures for Use of Data resulting from the use of UAS.

Effectiveness

The use of UAS is constrained to tactical cases and authorized purposes in the Standard Operating Procedures. The resolution of 720dpi is a good balance between image clarity and video file size.

PPB requires staff to be fully trained before being able to pilot a UAS and manage information collected from it. UAS are selected to withstand rain and wind, reducing risks of accidents or collisions.

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 will be lawfully deployed and not invade the privacy of individuals or observe 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.

UAS equipment will not be used to:

a) Conduct random or indiscriminate mass surveillance activities.

b) 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.

c) Harass, intimidate, or discriminate against any individual or group.

d) Conduct personal business of any type.

e) Crowd control/crowd management unless a life safety critical incident occurs.

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

Absent a warrant or exigent circumstances, Remote Pilots in Command (RPIC) are forbidden from intentionally recording or transmitting images of any location where a person would have a reasonable expectation of privacy (e.g., residence, yard, enclosure). Reasonable precautions should include, for example, deactivating or turning imaging devices away from such areas or persons during UAS operations.

RPIC and staff are required to adhere to all laws governing the use of airborne cameras and thermal imaging systems for searches.

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 about any person with a reasonable expectation of privacy.

a) RPICs should be aware there are restrictions on the evidentiary use of training images under Oregon Law.

b) All video recordings and photos will be retained in accordance with public records law, PPB policy, the PPB UAS program retention schedule and Oregon's Policies and Procedures for Use of Data resulting from the use of UAS.

The Specialized Resources Division commander approves and supervises flights. The SRD commander also independently audits or gathers information on any UAS deployment to ensure its validity and adherence to all rules and regulations, including privacy.

Open source

Not applicable

Artificial Intelligence/Machine Learning claims

None.

Privacy Policy (link)

ORS 837.300 Aircraft operation. Unmanned aircraft systems - https://www.oregonlegislature.gov/bills_laws/ors/ors837.html

Privacy risk

Medium. Some risks need to be mitigated.

Surveillance Tech?

Yes

Portland Privacy Principles (P3)

Data Utility

Data collected by PPB units is taken to gather evidence and used only to provide contextual and environmental information in criminal activity, crash scene events, and cases authorized by the Standard Operating Procedure.

Full lifecycle stewardship

This privacy impact assessment is limited to the UAS, and its Standard Operating Procedures includes airborne cameras and thermal imaging systems, but not the vendor type. However, regardless of the vendor, the storage, access, management, and deletion of evidence footage should comply with laws and regulations in the judiciary information system.

Transparency and accountability

PPB is documenting each 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

These fields are accessible via a public dashboard and downloadable in csv format.

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 regularly by the Specialized Resources Division commander.

Ethical and non-discriminatory use of data

Forbidden uses of the UAS equipment include:

- Conducting random or indiscriminate mass surveillance activities.
- Targeting 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.
- Harassing, intimidating, or discriminating against any individual or group.
- Conducting personal business of any type.
- Crowd control / crowd management unless a life safety critical incident occurs.
- Weaponization.
- Use in conjunction with any type of facial recognition technology.

Data openness

Portland Police Bureau has developed a publicly accessible dashboard with information collected about UAS flights and purpose. Data is open and updated frequently.

Equitable data management

No special considerations for equitable data management. However, having accessible data about flights, purpose, and location of operation enables more public transparency and groups to understand potential overuse of this technology in certain areas. These actions can prompt conversations with the City of Portland.

Automated Decision Systems

The UAS won't include any automated decision systems.

Consent.

The collection of data will be in response to criminal activity, crash events, or authorized tasks. No consent will be sought in those cases and the data will be collected in compliance with applicable law. 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.

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
T	I	1.1 Risks due to unauthorized data sharing. If data gets shared: - with other groups within the agency - with other agencies - with other jurisdictions - with apps and service providers - with service providers third parties	High	Unlikely	- Train staff on the policies for data sharing with third parties. - Perform regular audits on data. - Develop data governance policies for data collected or derived from the use of UAS - Use of data encryption as allowed by law	Medium
T	I	1.2 Risks due to capturing personal identity or recording the activity of persons.	Moderate	Unlikely	The Standard Operating Procedure already contains 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 SOP. - As much as possible, provide advance and ongoing notice that a UAS will be or 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
T	I	1.3 Risk of not providing reasonable expectation of privacy	Moderate	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 are 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.	Low

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
					2. Private clubs and religious organizations: a. Churches, synagogues, mosques b. Private clubs where members must pay dues. 3. 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 creating individual, collective, property, or any other material harm.	
U	I	1.4 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.	High	Possible	The use of UAS in operations is restricted to providing information and assisting ongoing searches in combination with officers and K9 units. - assure that officers, pilots, and other staff and contractors complete privacy awareness, civil rights and civil liberties, ethics, code of conduct. and any other related training. - The new Standard Operating Procedure (SOP) creates better control and supervision of the use of UAS by the Specialized Resource Division commander. This line of authority resolves a number of internal previous issues around internal oversight and management of equipment. - Create a process for remediation and public input in cases of impacts to 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. - Minimization of retention time of information not connected to any investigation is subjected to Oregon's retention laws. - Perform independent privacy impact assessments for individual sensors (visual, FLIR, Radar, etc.) and publish the	Med ium

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
					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. - Certain zones are already designated as restricted due to limits of using aerial vehicles close to the airport or certain facilities.	
U	I	1.5 Risk of information breach of sensitive of private footage or information collected during the operation of a UAS.	High	Unlikely	All evidence resulting from the use of UAS will be handled and stored in accordance with PPB evidence procedures, Oregon public records laws, and ORS 837.362 (Policies and Procedures for Use of Data). Supervisors need to keep routine access log revisions to identify any potential breach or risk.	Medium
U	I	1.6 Risk of unnecessary deployment of UAS in pacific public demonstrations. The sole intention of using UAS for gathering intelligence information in pacific public demonstrations may increase the potential of conflict and trigger mistrust reactions with police agents that may be deployed for monitoring any dangerous situation.	High	Possible	Teams operating UAS should announce and inform those inquiring at the beginning and during an operation, when feasible and reasonable, that the UAS deployment. Protection of property is triggered at request of the owner. The updated SOP is based directly on current state law on use of UAS by law enforcement. It explicitly prohibits the use of UAS during crowd control/crowd management situations unless a life-safety critical incident occurs. The SOP allows use of UAS in life-safety issues like shootings, vehicle attacks, explosions, dangerous fires, etc.; these events may occur during a crowd event. Property damage would not be considered “life-safety” unless it also involved a significant threat to human life. The public needs to have reliable access to report misuse and abuse of UAS deployments. Annual reports should include the type of reports, suggestions, and actions taken from this public input.	Medium
U	I	1.7 Risk of using a new type of sensor mounted on UAS not collecting footage, like stingray interceptors, Bluetooth sensors, or other 'man-in-the-middle' technology.	High	Unlikely	The use of different sensors mounted on UAS will be covered by other impact assessments. However, general collection of information by UAS in Portland Police Bureau operations is already covered by this updated Standard Operating Procedure	Medium

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
					and privacy and records laws that apply to operations of UAS in Oregon. The use of UAS is specified in the SOP. Any other use is not allowed and would be in violation of this policy.	
U	I	1.8 Risk from Intelligence gathering or spying. The risk is that officers might be tempted to use a UAS to gather information about people or groups without probable cause or a warrant.	High	Unlikely	Officers and pilots are limited to the authorized uses described in the SOP. The policy forbids the use of UAS from doing random or discriminate mass surveillance or crowd control.	Medium
U	I	1.9 Risk of using footage from UAS flights for purposes different from the original case.	High	Unlikely	The risk of officers finding an illegal or criminal activity unintentionally recorded by flying a UAS over private property, which could start a criminal investigation from that footage. Per Oregon laws and the Standard Operating Procedure, any information collected cannot be used to inform a separate investigation and cannot be used to establish reasonable suspicion or probable cause. Also, the SOP requires Remote Pilots in Control not to take separate events intentionally and all efforts should be used to avoid recording the area and protect people's privacy and property.	Medium
T	II	2.1 Risk of collecting information on physical areas meaningful to specific communities without consent.	Moderate	Possible	- The Remote Pilot in Control and officers in charge of operations are encouraged to question deployment of UAS particularly closer to important community areas like churches, mosques, or temples, schools, community centers, and other meaningful community spaces.	Medium
U	II	2.2 Risk of overuse of UAS on specific groups or neighborhoods	High	Unlikely	- The use of UAS is in response to ongoing criminal activities, investigations, or supporting Portland Police activities. Deployment of UAS on specific neighborhoods is the result of other causes and not an intentional deployment of this equipment. - All the deployments are accessible with an open data dashboard and raw information can be downloaded from the same mapping visualization page. Further analysis of demographic data could be correlated also in the form of open data.	Medium

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
U	II	2.3 Methods of reporting disproportionately impact specific groups or neighborhoods	Moderate	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. - Add equity review and data justice analysis to data collected and any produced reports. - Use accessible language to publish reports and dashboards.	Low
T	III	3.1 Risk of a privacy data breach or data related issue	High	Unlikely	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. - Constrain 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. - Keep consistency in making the annual report available to the public and reviewed and approved by Portland City Council.	Medium
T	III	3.2 Lack of trust due to third parties not authorized use of information.	Moderate	Unlikely	Certify third-party users and minimize external processing of data to avoid any misuse or potential of data privacy breach.	Low
T	III	3.3 Lack of transparency	High	Possible	Lack of transparency usually leads to a reduction of public trust and allowing misinformation streams to create narratives that damage public image. Transparency can be increased by: - Keeping existing open data dashboard[2] of flights and use of UAS up to date. Create a channel to receive public input and	Medium

[2] https://www.portland.gov/police/open-data/uascalls

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
					questions. Link to customer services and track responsiveness and quality of service. - Adding clear visual Identification of equipment and teams while in operation - Allowing digital identification in the form of Remote identifiers while in operation of equipment (https://www.faa.gov/uas/getting_started/remote_id/drone_pilots)	
T	III	3.4 Lack of oversight and credible audits	High	Possible	- Inform staff about internal audits and reports in a timely manner. Release of annual reports is expected at the release of the new SOP. Currently, the public can access updated information about flights and purpose of operations. - Include reputable and neutral third-party audits and release results. - Maintain 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
T	IV	4.1 Risk from lack of internal data protection	High	Unlikely	- Work with the City's information security office to ensure that information protection systems are in place. Release summaries of cybersecurity audits and reports according to applicable law. Privacy breaches can have different sources, including: - Operators of Remote Pilots in Command (RPIC) - Visual observers - Storage data after the event. Some recommendations to reduce this risk are necessary because these UAS are commercial grade and may not include a high level of cybersecurity compliance: - Develop equipment procedures that support operators and PIC access to information securely. - Make sure visual observers are out of range and at a secure distance from operators. - Make sure equipment and all radio transmissions are also protected, encrypted, and have robust cybersecurity measures. - Include cybersecurity measures to personnel access and other authorized use of information after the incident.	Medium

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
					- 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.	
T	IV	4.3 Risk of lower quality of service due to lack of training	Moderate	Unlikely	Ensuring 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 unlikely. However, incorrect readings or interpretations and errors in operation may greatly impact the use and results of UAS.	Low
T	IV	4.4 Risk of low quality of service (QoS) of equipment and other measurement errors	Moderate	Unlikely	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 by: - 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 or personally identifiable 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. - An important factor of QoS is the performance of equipment under rain, windy conditions, or in the dark. Equipment that is unsafe or unreliable should be decommissioned. This criterion has already been considered by the Specialized Resources Division (SRD) that maintains and manages use of UAS.	Medium

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
					- Regarding sensor QoS, verify performance measures like resolution, rates of data acquisition, encryption methods, and 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.	
T	V	5.1 Risk of misuse, abuse, or outside the authorized use	High	Unlikely	Use outside of 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. - Preventive and corrective measures of misused equipment are already scheduled by the UAS Remote Pilot in Command (RPIC) prior and after deployments. - 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	Medium
T	V	5.2 Risk of not conforming with Oregon Law	Moderate	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. UAS Remote Pilots in Command (RPIC) require meeting training and flight hours as directed by UAS supervisors. RPICs can be restricted or removed from the program for any deviation from training, flight or reporting requirements.	Low
T	V	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	High	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 ensure that operators have the proper certifications for flying and using the equipment. UAS flight altitudes are limited to between 100 and 400 feet, depending on restricted zones. Lower altitudes are required	Medium

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
					near the airport, where the Port of Portland may also impose no-fly zones. The use of UAS can be intimidating in neighborhoods with historical mistrust of authorities. In these cases, try to find alternatives to the use of UAS to the maximum extent possible.	
T	V	5.4 Risks coming from FAA UAS operation rules like: FAA has published 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	High	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. These risks are already mitigated by the mandatory training that UAS Remote Pilot in Command (RPIC) needs to take before they can operate this equipment. The FAA recommends: - Define response in immediate emergency situations, including those caused by equipment malfunction or weather conditions. - Report to FAA each time a UAS 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 UAS by the same individual - Transportation of hazardous material - Operation over human beings (most likely, crowds of people; estimate/use descriptors to illustrate crowd density) - Temporary Flight Restriction (TFR) violations - Objects dropped from UAS	Medium
T	V	5.5 Risks due to non-standard UAS operations like: - Operating low over the heads of non-participating persons. - Flying between vehicles or operating over a roadway in use - Chasing people or pets - Attaching a firearm or weapon to the drone	High	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 follow ORS Chapter 837 and any other applicable law and regulation. All these risks are already mitigated by the mandatory training that Remote Pilot in Command (RPIC) personnel need to take to operate a UAS. Supervisors must inspect equipment before and after operations to verify their integrity.	Medium

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
		- Injuries to people or damage to property				
T	VI	6.1 Risks of accidents, damage to public property, City property loss, staff injuries, public injuries.	Moderate	Unlikely	The City should have an insurance policy regarding compensation in cases of property damage. Operators, maintenance personnel, and Remote Pilots in Command (RPIC) are trained to minimize property damage, including the equipment and sensors themselves.	Low
T	IV	6.2 Risks of fines for non-compliance with FAA regulations or Oregon Law.	Moderate	Unlikely	This is a low-risk scenario. Make sure that certification and audits and documentation are up to date.	Low
T	VI	6.3 Risks of lawsuits and other liability due to misuse of UAS	High	Unlikely	Operating a UAS could make the City liable to lawsuits or compensation claims. Operators are trained to reduce such incidents and equipment is inspected before and after deployments.	Medium
T	VI	6.4 Risks of compensation due to damages from privacy breaches.	Moderate	Unlikely	Regular sensitive or private information is managed under the City's high-quality standards on cybersecurity. Digital evidence shall not be edited, altered, erased, duplicated, copied, shared, or otherwise distributed in a manner inconsistent with established evidence protocols utilized by the Bureau	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