BES: Small Unmanned Aircraft Systems (SUAS)

Privacy Impact and Risk Analysis

Released version

Smart City PDX

June 30, 2025

PRIVACY ANALYSIS REPORT

City of Portland Privacy Toolkit

WHAT IS PRIVACY RISK AND IMPACT ANALYSIS?

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

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

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

WHEN IS PRIVACY IMPACT ANALYSIS RECOMMENDED?

A PIA is recommended when:

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

WHAT IS IT INCLUDED IN A PRIVACY IMPACT ASSESSMENT?

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

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

Executive summary

The Bureau of Environmental Services is interested in obtaining drones to support their work. The purpose of the drones is to support two main processes in the Bureau of Environmental Services (Field services, engineering and maintenance) and support any relevant secondary uses.

For engineering, small, unmanned aircraft systems (sUAS) or drones will be used to survey areas on BES property to show work progress to third-party contractors/consultants. The video will be used to communicate progress to create plans with, or share identified issues with consultants.

For maintenance, drones will be used to identify gas leaks along pipelines using heat sensors (or other appropriate sensors or cameras), check the safety of rooftops, and check water tower infrastructure. Most flying of the drone will occur within BES owned property, but there are use cases where it may fly over public right of way areas or private property.

Secondary uses of drones are not excluded such as assisting with watershed restorations, river pollution monitoring, sewer repairs, waste-water treatment plant security, and other relevant tasks conducted by BES.

Main risks include safety risks from flying near gas leaks, legal risks from improper use, and privacy risks from privacy invasion, no notification or consent, improper data handling, or excessive data collection.

These risks can be mitigated by using fair information practice principles for data handling, providing notification or an avenue for consent where necessary, creating flight paths and no fly zones, and practicing data minimization by recording only when necessary.

Risk area	Risk level	Highlighted risks
Individual Privacy Harms	Low	The main privacy harm that can occur is the recording of community members in areas where they have an expectation of privacy or in public. The risks that contribute to this harm are the Inappropriate or unnecessary collection of personal information, aerial trespassing, data breach, and risk of ineffective drone policy. This risk is low because the primary use of sUAS is maintenance and monitoring infrastructure, and not to surveil people.

Risk area	Risk level	Highlighted risks
		Mitigations include recording procedures to limit filming to only necessary recordings, charting clear flight paths and avoidance zones for flights outside of BES property, avoid turning away from BES property while recording, proper data management and security, and effective drone policy.
Equity, Disparate Community Impact	Low	This risk is unlikely because of primary use of drones tend to be located on BES property, but in the case that filming or flying is done around homes, there is a chance that these homes will be inequitably at risk of accidental surveillance.
Political, Reputation & Image	Medium	Risk of a lack of transparency can create reputation harm to the City of Portland. The City should provide notice and inform neighbors about the use of sUAS. Other strategies can include visually identifying drones by bright colors, planned flights can be posted online in advance and having a dashboard keeping a history of the use of drones, like the one created by Portland Police.
City Business, Quality & Infrastructure	Medium	Risks of cyber-physical (Jamming communication and vandalizing or shooting) attacks to these devices and ensuring safe use in high-risk environmental conditions like checking for leaks in gas lines.
Legal & Regulatory	Low	There is a risk of lawsuits based on privacy torts, UAS law, and data breaches.
Financial Impact	Low	Risks that contribute to financial harm to the City of Portland or to the community are property damage, fines from noncompliance with UAS law, and the cost of UAS replacement or parts replacement from wear.

Privacy Analysis

Purpose of the technology, project, data sharing or application

The purpose of the drones or small Aerial Unmanned Systems (sUAS) is to support the Bureau of Environmental Services' (BES) employees in their work including building or construction progress, infrastructure integrity, watershed restorations, photography, river pollution monitoring, and wastewater plant security.

The engineering staff has requested using drones to survey areas on BES property to show progress to third party contractors/consultants. Maintenance staff would use drones to identify gas leaks along pipelines using heat sensors and other technology.

BES has field staff who work on privately owned roofs regularly to check monitoring equipment. They have no way to check roof conditions until they are already on the roof. Using a drone to locate any fall protection devices first will ensure safe work conditions and allow them to proceed with their work.

BES security and field staff will use sUAS to view and monitor remote locations. Often, they are lone workers in an area of dangerous terrain. It would be a lot safer if they could use drones to see if there are blockages at pipes or detect unsafe conditions in ravines or other natural areas.

Information and use of sUAS may be shared with other City bureaus, particularly with the Water Bureau.

Name of the entity owner of the application and website

Bureau of Environmental Services (BES)

Type of Organization

Public

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

Data

- Video and images of sites and pipelines
- BES Staff, likely, will be filmed
- Community members may be filmed

Sources

- Visual pan-tilt-zoom (PTZ) Camera
- Thermal cameras
- Passive Infrared (PIR) cameras

- Other cameras (e.g., panoramic, 360, etc.)

How personal data is collected.

Personal data, if it is collected, will be collected using cameras. Personal data is not the technology objective or project's objective. If any other camera is used, such as a thermal or infrared, there will be a certain level of obscurity around who an individual is exactly, but perhaps not around what they are doing.

Given that there is a chance that drones can be flown within view of a house or apartment, there are certain applicable privacy tort laws and Oregon UAS law. The Oregon invasion of personal privacy tort applies if (put crudely) someone knowingly recorded another in a state of nudity where an individual has a reasonable expectation of privacy, or if someone disseminates these images/recordings. [1]

Who can access the data?

BES staff. Consultants, if video recordings are retained, can view or access them (formal process is not set).

Purposes the data is used for.

The data could be used for a wide range of purposes related to the Environmental Services, however, mainly engineering and maintenance. Data, if retained, will be used to support these projects.

Where the data is stored.

On City of Portland servers, or on third-party information management servers.

How data is shared.

Data/Video can be shared through teams or through email, if retained.

How long is the data stored?

ORS 837.362 Drone policy is required, and it must include/disclose data retention times and a policy for intergovernmental data sharing. [2]

Data retention length depends on its classification and applicable City policy. If it's used for aerial photography or for photography generally meant to document projects, it may be kept permanently. If images are considered technical project records, then it may be kept up to 10 years after the project's completion. For additional contingencies see the Bureau of Technology

[1] https://oregon.public.law/statutes/ors_30.831
[2] https://www.oregonlegislature.gov/bills_laws/ors/ors837.html

Services retention schedule in sections "Engineering and Construction" and "Environmental Services." [3]

Effectiveness

Drones are most likely the best tool for dangerous places and tasks, such as identifying leaks in pipelines at scale, in hard to reach or unwelcoming areas, or high places. The effectiveness of the camera for fugitive emissions largely depends on whether the camera is made to detect the necessary gas and the resolution of the camera. If the camera does not detect the target gas it will not be effective, and the risk of collecting personal information may outweigh the benefits. For example, a thermal camera may not detect all kinds of gas, so an infrared camera may be a better tool or a combination of both.

Necessity & Proportionality, Fundamental Rights, and Consent

Necessity and Proportionality

Our use of the term “Proportionality and Necessity” refers to whether the means of collection and the data collected are necessary to complete a specified aim, that is, not collecting, retaining, or sharing more information than necessary to support engineering and maintenance; and to consider if there are less intrusive but equally effective ways to complete a specified aim, that is, analyze whether the technology is proportional to the objective. Technology could be said to be proportional if the data used does not pose an outsized risk compared to the benefits gained from technology.

Drones are not necessary to conduct the two use cases, but drones are an incredibly helpful tool because of their ability to offer a view from height and greater coverage. Additionally, the benefits gained such as time, safety, and image quality make the use of drones reasonable and proportional.

There are other methods of collecting ariel imagery such as planes, helicopters, or even satellites. One previous alternative of collecting aerial images of building progress or land use was by flying a plane over the area and then snap pictures. It’s clear that the drone does not require coordination with an external entity for a plane and a pilot. It also carries the same amount of risk of unintentional surveillance/personal information capture and potentially intrusion on seclusion.

Other methods for checking gas pipelines could place individuals in danger. For instance, simply using a gas detecting camera from a distance must be done from a cross wind or up

[3] https://www.portland.gov/auditor/archives/retention-schedules
https://oregon.public.law/rules/oar_166-200-0370
https://oregon.public.law/rules/oar_166-200-0355
https://www.portland.gov/service-areas/public-works

wind position, or else assessors may inhale gases. Or another method may include wearing Personal Protective Equipment and detecting gas by hand. There are safety risks in flying drones near potentially leaking gas pipes, however, mitigations of this risk fall outside the scope of this assessment. Consider a procedure to prevent any ignition of gases.

Fundamental Rights

These drones are not expected to have a direct effect on the community's fundamental rights, because the uses for the drones are limited to engineering and maintenance in BES owned areas. These drones are not meant to perform surveillance on people, especially community members. The inherent maneuverability and height advantage drones offer for surveying also, unfortunately, makes them a great tool for inadvertent or unintentional surveillance and personal data collection.

The City should consider ways they can avoid inadvertent surveillance from occurring. For example, and only for example, inadvertent surveillance could occur when drones used to look for gas leaks, but operators, while flying the drone near apartments or homes, accidentally record someone in their apartment or home. One could imagine this occurring during protests or where surveillance can be seen as an affront to rights such as assembly or speech--not only affecting a right to privacy but right to assembly.

Consent

There are no regulations that require the City to obtain consent from and give notice to community members if the drone is flown over BES property. However, there may be consent implications if drones are flown over homes and private property.

Depending on how close the drone intends on flying near a community, it may be worth notifying them about its use generally or acutely (for instance, in the very off chance that there is a part of a suspect gas pipeline that runs near a single home). To uphold our values as a City and uphold laws (if applicable), consent should be obtained before any flying is done over private property. [4]

Privacy safeguards

- Limit collection of data
- Limit use of data
- Limit retention of data
- Avoiding areas where individuals have a reasonable expectation of privacy
- Limit use of drone for security around BES property
- Transparency and Accountability Mechanisms

Open source

N/A

[4] https://www.oregonlegislature.gov/bills_laws/ors/ors837.html

AI/ML claims

No.

Privacy Policy (link)

It depends on the vendor.

Surveillance Tech?

Yes. The main purpose of the use of sUAS by BES staff is not surveillance, but the collection of information can include unintentional recordings of people and campsites.

Portland Privacy Principles (P3)

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

The drones support important projects that community members may not think about often but enjoy the consequences of.[5] If a gas pipe were to leak, there is a chance that it may harm community members surrounding the area either by the diffuse effect of emissions in the air the City of Portland collectively breathe, or if there is ignition of these gases. Communication between the bureau of environmental services and their consultants is important in performing work that benefits the community at large. Retaining aerial photography of projects and landscapes provides a historical record for the City. Consider whether it is worth recording video, for example, keeping footage of pipelines only, only start recording once a leak is discovered, or even not recording during take-off or touch-down.

Full Lifecycle Stewardship: Data, Metadata and Information will be secured and protected throughout its life cycle. That includes collection, storage, use, control, processing, publication, transfer, retention and disposition.

The project should follow a standard procedure for cybersecurity and necessary procedures for drone cyber-physical security.

Data Lifecycle Stewardship

- Collection
    - Consider editing video or blurring
    - Consider whether the video is worth collecting, particularly for gas pipe inspection
- Use
    - Don't share for other purposes, especially if footage contains personal information of individuals (e.g., faces, nudity, names).
- Disclosure
    - Don't disclose to other entities other than consultants and internal bureau staff, unless necessary (e.g., subpoena, public record request).
    - Ensure video does not contain personal information before sharing with consultants.
    - Notify consultants to avoid further sharing or copying.
- Retention
    - Retain information as short as possible.
    - Archive if necessary pursuant to City regulations.
- Deletion
    - Ensure deletion of video after retention or archival periods.

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

Transparency

Public notice to community if aware of the drone's route.
Consent, if necessary, before flying near sensitive or private areas.
Consider a dashboard or other transparency tool for drone use but be aware of the potential to share confidential city information.

Accountability

Accountability is practically equivalent to the idea that there ought to be technological, administrative, or legal structures in place to make sure that the drones are doing what they are supposed to be doing. The Bureau of Environmental Services is working on a drone policy that should include accountability measures such as a manager or person(s) in charge of privacy (e.g., consent, inform, data collection minimization, video editing, video blurring), data governance measures, flight paths, proper filming techniques, or other content not ideated here.

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

The two main use cases of BES's drones or sUAS are engineering and maintenance; however, there are downstream decisions made under each umbrella. These decisions may have an ethical impact on community members, but it's hard to foresee what these unethical impacts may be. Symmetrically, there are equity decisions made under these two umbrellas. It's advisable to lean on the equity professionals where possible when making decisions that impact people based on the information gained from drones.

Data collected from the drones will most likely contain images of land, however there is an off chance there will be an image of a person. For this reason, the ethical handling and non-discriminatory handling of this data is important. However, it's unclear where there may be discrimination.

By following fair information practice principles (FIPPs), especially use limitations, data minimization, and providing notices, the City can hope to avoid many privacy issues—likely mitigating more than one risk with just a few FIPPs (see mitigations).

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

Depending on the classification of Data it may be shared publicly. Video could be used to provide transparency to community members about public interest projects or some other positive use of video given there is no personal information within it.

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

There are minimal equity impacts by using these drones, but the City should take care of using drones outside of BES property.

Automated Decision Systems: The City will create procedures for reviewing, sharing, assessing, and evaluating City Automated Decision System tools -- including technologies referred to as artificial intelligence -- through the lens of equity, fairness, transparency, and accountability.

There is no use of automated decision systems in this project or technology.

Privacy Impact Risk Severity Assessment

WORST CASE SCENARIO	Medium

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

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

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
U	I	1.1 Inappropriate or unnecessary collection of personally identifiable information (PII) and recording of community members	Moderate	Unlikely	There is a risk of collecting faces or other PII of community members. A pilot could simply turn the drone toward a community to figure out where it's located and then capture video of community members. Some mitigation measures include editing video, so PII is removed or to not record until necessary. Drone operators can also flag flights where they may have spotted a community member, indicating that some editing or blurring may be needed later. The type of camera impacts the likelihood of this occurring. If it is a 360-camera, the risk of unnecessary video collection increases dramatically. Consider charting clear flight paths and avoidance zones for flights outside of BES property and avoid turning away from BES property while recording.	Low
T	I	1.2 Risk of aerial "trespassing" and recording on private property without authorization.	Moderate	Unlikely	Flying over or near private property increases the risk of invading people's privacy or intrusion of seclusion. However, it also breaks an unspoken rule, that is, not disturbing people unnecessarily. This disturbance harms people by taking their time to assess the situation of marked or unmarked drone flying by their home. The City may want to consider developing an approach to how they traverse pipelines or generally fly in areas near the edge of BES property, if needed, that offers homeowners space, and if such space is not available provide notice and a public feedback mechanism or go about it another way (perhaps on foot with PPE). A notice mechanism can take the form of knocking on their door or providing some kind of messaging.	Low

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
					Additionally, the City may want to consider placing some marking on the drones so someone may gather who owns it and not assume that it's hostile.	
T	I	1.3 Risk of misusing video or using video in ways not in drone policy	Moderate	unlikely	Some uses of video are appropriate and push the progress of a BES project forward. Some uses of video are inappropriate and risk harming individuals and the City of Portland. The cross section this risk highlights are those uses that are inappropriate and not in the drone policy (in uses or forbidden uses). If the use of the drone is helpful but not in the drone policy, some administrative process may be required like an approval from someone. Supervisors need to be trained to verify appropriate use of drone footage collection and access.	Low
U	I	1.4 Risk of authorized third parties obtaining and sharing footage containing images of community members	Moderate	unlikely	With the assumption that images of community members were collected and retained by BES, there is a risk of sharing this kind of information. Mitigation may include those preventing images of community members from collection but additionally notifying consultants or third parties that they ought to refrain from further sharing. There also should not be any attempts to identify community members if their image happened to be collected by the drone.	Low
T	I	1.5 Risk of drone for other uses	Moderate	Possible	This risk can represent a couple of cases of using drones for other purposes: a. BES may expand the use of drones for other purposes from the original plan. b. A drone is used intentionally for other purposes without the bureau authorization. BES is developing a policy to use drones. This policy needs to have limitations on the authorized uses of drones in the bureau. The City of Portland may develop similar policies for citywide use.	Low
T	I	1.6 Risk of data breach	Moderate	Unlikely	Data breaches may occur when there is unauthorized copying, sharing, or deletion of video from servers. This action can be done intentionally or unintentionally. The staff working on this project must follow cybersecurity training and procedures on how to avoid data breaches in the City. In case	Low

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
					of an incident involving a data breach, the bureau needs to report immediately to the information security group at the Bureau of Technology Services.	
U	I	1.7 Risk that the drone policy misses privacy protections.	Low	Possible	There is a risk that the drone policy does not protect from privacy harms, primarily because it's difficult to forecast all possible future cases of privacy harm. To mitigate policy changes or privacy loopholes, implement effective supervisory tasks, oversight, and reporting that can help documenting issues and include them in future policy updates.	Low
T	I	1.8 Risk of releasing unblurred personal identifiable images.	Moderate	Unlikely	Public records request of footage may include video or still images of people's faces, license plate numbers, or any other sensitive information. This information may need to be blurred or redacted to comply with laws or privacy concerns. Public records officials at BES need to be aware of this risk and be prepared with the proper tools for video editing that assist them in finding these sensitive images or information and blurred sensitive information in public released files.	Low
U/T	II	2.1 Risk of intimidating individuals due to the use of sUAS in their proximity.	Low	Unlikely	The likelihood of flying over or near homes is low, and it's unclear whether most of these homes are owned by low-income households or by those in at-risk communities, but if BES does fly near homes owned by these communities, the City runs the risk of inequitable impact. Additionally, areas around BES property tend to be areas in which these at-risk communities live, then the City runs the risk of inequitable surveillance. Seeing a drone flight in proximity can be an intimidating event for many. Particularly if they are not aware of their purpose or have negative experience or perceptions of these devices. Proactively informing the public about the use of these devices in their vicinity will prepare people and reduce inequitable impacts. Clearly identifying drones with visual clues describing ownership and purpose can assure responsible use of this technology and lower anxiety and fears against this technology.	Low

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
T	III	3.1 Risk of public mistrust due to the lack of transparency	Moderate	Possible	The lack of information before, during, and after a drone operation creates a sense of mistrust and intrusiveness, even in cases where these devices are not being used for surveillance operations, but just for building or infrastructure maintenance. Using drones close to homes or apartments could raise eyebrows of homeowners or tenants about the use or policies regarding drones. Without notice, they may assume that drones are there to surveil them. Consider adding a page on the BES website on portions of the drone policy along with a general announcement that BES will be using drones. Also, given that the use of drones by BES are planned and scheduled operations, some advice notice of these operations can be shared online. The use of open data dashboards that describe locations, time, and purpose of the use of drones add more transparency. Portland Police Bureau has already developed their own sUAS dashboard[6] that could be replicated in other bureaus. Work with the 311 program and provide with enough information and contacts within BES to respond promptly to queries from the public. Finally, a clear visual identification of a sUAS can identify a device owned by the City and their purpose. This can be done either by color code or an identifying pattern. Drones already need to have remote ID numbers to comply with FAA regulations[7].	Medium
U	III	3.2 Risk of mistrust due to a lack of authority, accountability, or oversight.	Moderate	Unlikely	Drones or sUAS are devices that are perceived as intrusive in the public view and responsible use need to include clear description of responsibilities, oversight, and accountability measures. Consider creating a channel of communication from community members to BES and ultimately to drone operators and managers.	Low

[6] https://www.portland.gov/police/open-data/uascalls
[7] https://www.faa.gov/uas/getting_started/remote_id

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
U	III	3.3 Risk of data loss due to poor data management	Low	Unlikely	If the City is not able to account for all instances of video or data collected from drones, it runs the risk of its disclosure or unauthorized access, along with data duplication or unauthorized destruction. Consider a data management protocol that accounts for each recording and any backups along with any metadata and their retention times.	Low
T	III	3.4 Risk of low quality of service (QoS) of equipment and other measurement errors	Moderate	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, BES needs to make sure that data is properly secured, stored, and disseminated by: - encrypting the transmission of UAS video. - restricting access to real-time videos to authorized users with a need to know. - restricting disclosure of analytical products that contain UAS-obtained images to approved requesters and redacting personally identifiable information and other sensitive information prior to disclosure unless the requester has a need to know.	Medium
U	III	3.5 Risk of misusing sUAS in emergency situations	Moderate	Unlikely	In emergencies, BES may need to use sUAS outside policy or authorized purposes. This exemption allows the City to respond and resolve unique issues that the City of Portland may face. This scenario may open the possibilities to unaccountable actions. During an emergency, the use of sUAS must be documented and reported to the public once the emergency has ended.	Low
T	IV	4.1 Risk of drones being struck down by people	Moderate	Unlikely	There have been instances of this occurring throughout the US, particularly in municipalities and companies' drones checking power lines near homes; or where a drone is flown over a person's home numerous times unannounced. (include signal jammers) A mitigation for this is to inform necessary stakeholders.	Medium

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
					Crimes involving unmanned aircraft systems are defined by Oregon law: https://oregon.public.law/statutes/ors_837.995	
U	IV	4.2 Risk of drones causing explosion	High	Rare	Given that there is a large enough leak and there is some spark or another causal thing that creates ignition of fugitive emissions, a fire may occur. The impact of this combustion may be large, and the remediation measures and down time depend on its size.	Medium
T	IV	4.3 Risk of cyberattacks	High	Unlikely	Along with data breaches, drones are susceptible to cyber-physical attacks from bad actors. This can include jamming communication signals and trying to intercept and control a flying device. Some mitigations of cyberattacks are to update the drone's firmware, use strong passwords, use anti-virus software, and use the "Return to Home" (RTH) mode to ensure drone recovery. https://www.cisa.gov/topics/physical-security/be-air-aware/uas-cybersecurity Portland's Information Security Admin Rule. https://www.portland.gov/policies/technology-services/information-security/bts-201-information-security-administrative-rule	Medium
T	IV	4.4 Risk of physical damage or vandalism to the sUAS	High	Unlikely	sUAS can be vandalized or physically attacked with the purpose of taking them down. Vandalism and other attacks like gunshots are possible and it would be impossible to predict when an incident like this can happen. It is important to assess the level of safety in the surroundings of the sUAS operation before deploying the device. If an incident happens, it is important to report on the event and ensure the safety of staff operating the sUAS.	Medium
U	I	4.5 Risk of misusing drones	High	unlikely	Drones are primarily used for engineering and maintenance along with additional tasks directly related to environmental services. However, the use of drones for anything unrelated to environmental services poses a risk of harm or wrong to community members and poses a risk of violating our own policy or values. Supervisors need to keep regular logs and records of flights and have this information available for potential audits or even public release of this information.	Medium

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
					An annual report on drone use can also create more transparency and provide information to the public about any possible abuse if any.	
U	V	5.1 Risk of lawsuit due to privacy harms from community members	Moderate	Unlikely	Community members may sue the City based on privacy torts, data breaches, or other laws about drone use. Privacy torts consist of intrusion on seclusion and public disclosure of private facts. Operating a UAS could expose the City to lawsuits or compensation claims. Operators are trained to reduce such incidents, and equipment is inspected before and after deployments. Don't collect information in locations where individuals have a reasonable expectation of privacy such as bathrooms, locker rooms, backyards, any area where a person undresses. Action by Owner of Real Property. https://oregon.public.law/statutes/ors_837.380 Operation over privately owned premises. https://oregon.public.law/statutes/ors_837.370 sUAS and their pilots should have their registration and appropriate training to operate the devices.	Low
U	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 with 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. Weaponizing of unmanned aircraft is forbidden with certain exemptions: https://oregon.public.law/statutes/ors_837.365	Low
U	V	5.3 Risk of not complying with public records request	Moderate	unlikely	Community has a right to information through public records requests, if the City fails to provide necessary records, then they fail to uphold that right.	Low

B	RT	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
T	VI	6.1 Risks of accidents, damage to public property, City property loss, staff injuries, public injuries.	Moderate	Possible	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. Mitigation of this risk includes proper training of pilots and system operators, proper maintenance and operation checks before and after every flight, and valid insurance that covers these types of incidents.	Low
T	VI	6.2 Risks of fines for non-compliance with FAA regulations or Oregon Law.	Moderate	Unlikely	There are fines if the City does not follow FAA regulations. Make sure that certification and audits and documentation are up to date. The project supervisor must ensure that the equipment, pilot, and operations are all in compliance with FAA and any other applicable regulations.	Low
T	VI	6.3 Risk of higher costs of replacement of drones because of vandalism, wear and tear	Low	unlikely	It is reasonable to assume that, after some time, issues with the device may occur due to either wear or vandalism. Equipment should keep proper maintenance and records that include flight logs, pilots' records, maintenance tasks, and any other documentation that registers incidents and compliance activities.	Low

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 on 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 a 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	It is likely to occur yearly
Likely	Likely to occur every 2 years
Possible	Likely to occur every 5 years
Unlikely	It is likely to occur every 10-20 years
Rare	It 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 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 underpinning 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 data collection.
Privacy safeguards	Measures are 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 belief that automated processing of the loan may not consider the unique situation of the customer.
Right to be forgotten	Also known as the 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 a 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