OFFICE OF THE
STATE AUDITOR

Comment Period: In an effort to make our publications accurate and useful to our intended audience, we invite individuals who work for and with government entities to read this draft and provide comment. The comment period will end January 16, 2025. Comments should be submitted to Nora Kurzova at nkurzova@utah.gov.

Privacy Alert 2024-05 - DRAFT

Date: December 16, 2024

Subject: Privacy and Security Risks of Using Drones

Introduction

The State Privacy Officer provides recommendations for local government entities to reduce the privacy and security risks of using unmanned aircraft systems (UAS); more commonly referred to as drones. These recommendations reflect input provided by the Cybersecurity and Infrastructure and Security Agency (CISA), as well as the recently legislated Utah Aeronautics Act.

Background

While drones offer numerous benefits, such as faster response times in search and rescue operations, enhancing officer safety before entering crime scenes, and conducting inspections efficiently, they also pose significant risks like unauthorized **data access** and **data loss**. These concerns are especially relevant when using drones from companies based in countries where governments could persuade or require manufacturers to provide access to sensitive data. This data might include images and videos of critical infrastructure vulnerabilities or reveal the habits of users and subjects, leading to increased privacy risks if shared without proper controls.

Upcoming Legal Requirements

The Utah Aeronautics Act (*Utah Code* 72-10-1202) part 12 states that, as of January 2025, Utah government entities or contractors in Utah **may not use drones/UAS for inspecting critical infrastructure**[1] if the devices are manufactured or assembled by a covered foreign entity,[2] **unless** the following conditions are met:

1. **Non-Internet Connection**: The UAS is not connected to the internet during the inspection.

[1] Inspection would typically be a targeted activity focused on reviewing the infrastructure specifically, as opposed to a "fly by" or seeing the infrastructure in the background. Consult your legal counsel for further guidance.

[2] "Covered foreign entity" means an individual, foreign government, or party: 1. On the Consolidated Screening List or Entity List as designated by the United States Secretary of Commerce; 2. Domiciled in the People's Republic of China or the Russian Federation; 3. Under the influence or control of these governments; or 4. That is a subsidiary or affiliate of such entities.

2. Data Handling: Any data collected (e.g., images, video, geospatial data, flight logs) must be removed before reconnecting to the internet.

3. Video Broadcast: If broadcasting video through an internet connection (outside of the inspection of critical infrastructure), the software must be developed in the US or approved under the National Defense Authorization Act.

Recommendations to Reduce Risk to Privacy and Security

The State Privacy Officer recommends the following considerations in reducing the risk to privacy and security when using drones:

1. **Use a Secure by Design Drone**: Choose drone with built-in security features from reputable vendors.
2. **Implement a Zero Trust Framework**: Restrict access to critical data and systems, limit connectivity where needed or required by law.
3. **Regular Software Updates**: Keep all firmware and software current.
4. **Data Protection Measures**: Encrypt data and minimize exposure before, during, and after drone operations.
5. **Evaluate Foreign-Manufactured Drones**: Be cautious of potential security risks from foreign-made UAS. These may fall under the "covered foreign country" rule.
6. **Train Personnel**: Ensure personnel operating the drone are adequately trained in privacy and security.
7. **Conduct Privacy Impact Assessments (PIAs)**: Perform assessments before using drones to identify and mitigate potential privacy and security risks.
8. **Video Broadcasting:** After the assessment, any broadcast or transmission of collected data must be done using secure, US-developed or NDAA-approved software, and not any pre-installed or pre-loaded software from the UAS.

Conclusion

Utah government entities need to be aware of both the benefits and potential risks of using ever-evolving technologies. Information from these technologies may create risks to both U.S. national security and the privacy of individuals. All Utah government entities should consistently implement strategies to mitigate security and privacy risks by January 2025.

References/Resources

CISA Cybersecurity & Infrastructure Security Agency
CISA January 2024 Guidance
S.B. 135 (2024)
Privacy Toolkit