TOOLBOX TALK: Privacy and Data Protection Awareness

RATTLIR Safety Series – "Strike Before It Bites"

Purpose

This toolbox talk provides awareness of privacy responsibilities, data protection requirements, and cybersecurity expectations when operating drones in industrial, utility, and critical-infrastructure environments. RATTLIR's operations rely on NDAA-compliant, U.S.-manufactured aircraft such as the Inspired Flight IF800 Tomcat to ensure secure data handling, eliminate foreign telemetry risks, and uphold client confidentiality.

Privacy Considerations for Drone Operations

Protecting public, employee, and client privacy is essential to ethical and compliant drone operations:

- Avoid capturing unnecessary imagery of individuals or personal property.
- Never collect or store personally identifiable information (PII) unless required by the mission.

- Follow flight paths that avoid residential areas when inspecting utilities or linear assets.
- Blur or remove identifying features during post-processing if incidentally captured.

Data Protection and Cybersecurity Requirements

RATTLIR enforces strict data handling practices to safeguard sensitive infrastructure information:

- All flight imagery, thermal scans, and mapping data are stored on encrypted, locally controlled devices.
- No data is transmitted to foreign servers, unapproved cloud services, or unknown telemetry endpoints.
- Operational copies of imagery are retained only as long as necessary to fulfill client agreements and internal quality assurance requirements.
- Data is transferred through secure, client-approved channels using encrypted file systems.

NDAA Compliance and Platform Security Expectations

RATTLIR exclusively uses NDAA-compliant systems such as the Inspired Flight IF800 Tomcat. These aircraft meet DoD cybersecurity expectations and avoid prohibited foreign components, reducing exposure to telemetry leakage, firmware compromise, and external command-and-control risks.

- NDAA-compliant aircraft avoid components from covered foreign entities.
- Blue UAS platforms undergo DoD-level cybersecurity vetting.
- RATTLIR drones do not auto-sync to any cloud service or external accounts.
- Using secure aircraft sets RATTLIR apart from competitors who operate non-compliant systems.

Protection of Critical Infrastructure Data

Drone imagery of industrial sites must be protected due to its potential security implications:

- Substations, transmission corridors, pipelines, and power plants require heightened data sensitivity.
- Unauthorized distribution of imagery may expose vulnerabilities or system configurations.
- Flight logs, thermal scans, and defect images must be shared only with authorized client personnel.

Emergency Response for Data Exposure Events

If data exposure, device loss, or suspected compromise occurs, immediate action is required:

- Notify RATTLIR leadership and the client immediately.
- Isolate affected storage devices and prevent further access.
- Document what data may have been exposed.
- Implement RATTLIR's secure data-containment procedure.

Discussion Questions

- Do you understand why RATTLIR uses NDAA-compliant drone platforms?
- Are you aware of your role in protecting sensitive imagery and client infrastructure data?
- Do you know the proper procedures for reporting a suspected data compromise?

RATTLIR Takeaway

RATTLIR protects privacy and critical infrastructure by combining secure flight operations, NDAA-compliant aircraft, and disciplined data handling practices. By controlling where data flows, who accesses it, and how it is stored, RATTLIR strikes before it bites – preventing data exposure, safeguarding clients, and maintaining the highest professional standards in the sUAS industry.