CIO ASSOCIATION OF CANADA

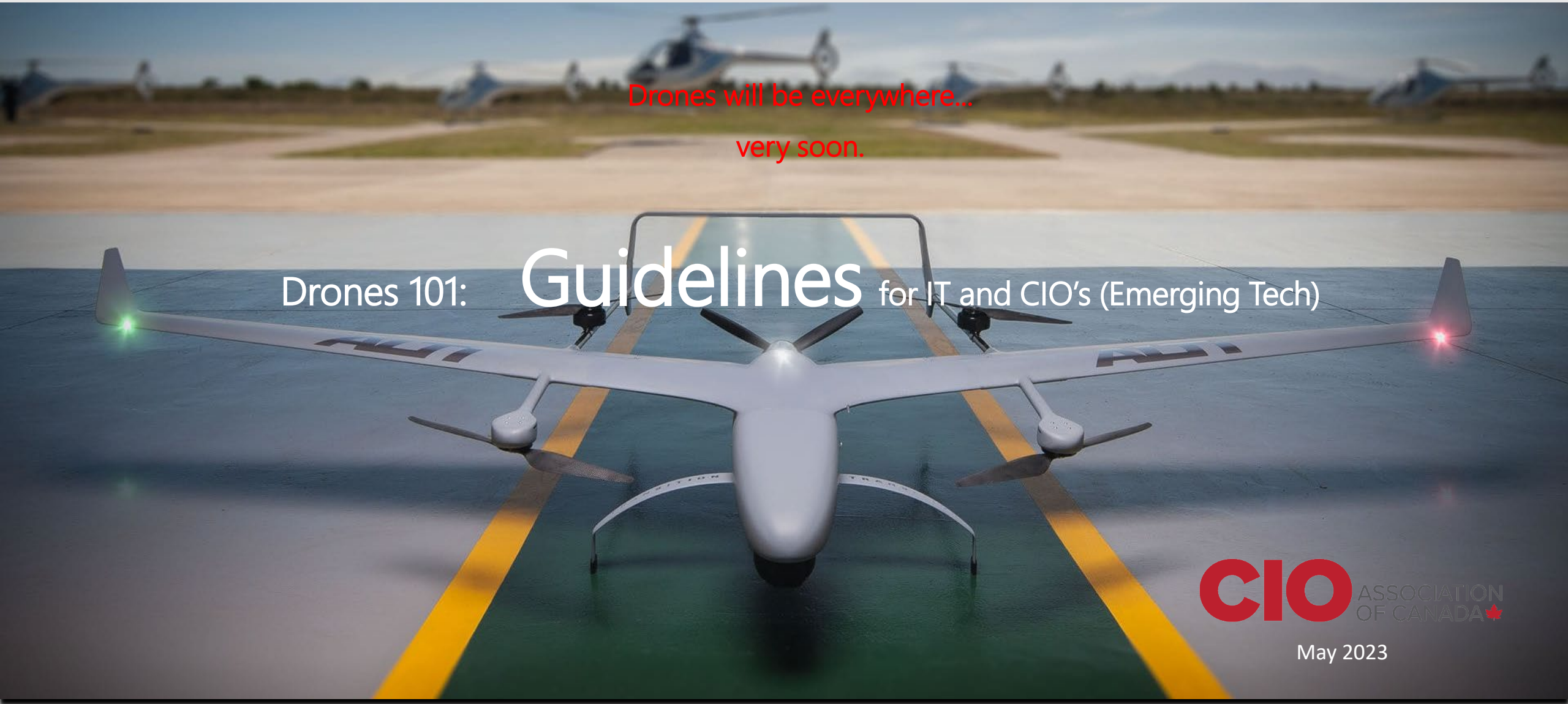
2023 CIO PEER FORUM

BREAKOUT SESSION L:

DRONES 101: GUIDELINES FOR IT AND CIO'S

EXO DRONE

Presentation



Drones 101: Guidelines for IT and CIO's (Emerging Tech)

CIO ASSOCIATION OF CANADA

May 2023

EXO DRONE

DRONE REGULATION IN CANADA

What is regulated?

As soon as you use a drone that weighs more than **250 grams**, you are subject to Part IX of the *Canadian Aviation Regulations* (CARs).

Impact for the pilot?

1. Registration of your drone with Transport Canada (5$)

2. Obtain one of the two (2) available pilot certificates
   - Getting a *Drone Pilot Certificate – **Basic Operations***
   - Getting a *Drone Pilot Certificate – **Advanced Operations***

What is the difference between a <u>basic</u> and an <u>advanced operation?</u>

First, you need to know your "**<u>drone category</u>**"

DRONE REGULATION IN CANADA (continued)

DRONE CATEGORY ? You only have three (3) questions to remember...

1. Do I want to use my drone within 30 meters (100 feet) of a person who is not part of my team (co-workers, friends, etc.), in short, a human who does not know that a drone flies in the air

2. Do I want to use my drone inside a controlled airspace? (With air traffic control approval - Navcanada.ca/rpas)

3. Do I want to use my drone within 5.6 kilometers (3nm) of an aerodrome certified in the Canadian Flight Supplement (CFS) or a military airport?

If you answered "**YES**" to any of these questions, you are conducting "**Advanced operations**" in the eyes of Transport Canada.

If not, you are doing "**Basic Operations**".

DRONE REGULATION IN CANADA (continued)

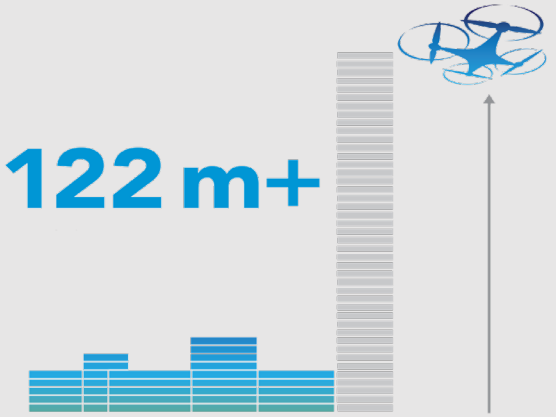
I would like to conduct even more complex drone operations ?

You will need a *Special Flight Operations Certificate*, better known as **SFOC**, to fly:

- At an advertised event

- A drone over 25 kg

- Above 122 meters (400 feet)
approximately a 30-storey building



Flights Beyond Visual Line Of Sight (BVLOS) are also subject to a Special Flight Operation Certificate (SFOC) application.

The more complex your operations are, in the eyes of Transport Canada, the more your SFOC application must be based on a robust operational structure based on risk analysis

(Operations Manual)

DRONE REGULATION IN CANADA (continued)

MANDATORY DOCUMENT MANAGEMENT

You must keep the following records:

(a) Name of pilot, crew members, flight time for each flight or series of flights;
(b) Technical record of your SATP;
- Names of the people who performed the maintenance;
- The date of the maintenance;
- For modifications, manufacturer, models and description of parts installed
- Instructions provided for performing the work.

Retain your records so that they are available to the Minister, upon request
- 12 months for records referred to in paragraph (1)(a);
- 24 months for records referred to in paragraph (1) b)

If you sell your drone, you must provide the purchaser with all those records

ADDITIONAL CONSIDERATIONS

TECHNICAL ASPECT OF DRONES RELATED TO IT SECURITY

Drones (or uAV's) are flying computers equipped with cameras and sensors that collect data. As such, these are the main aspects we think you need to address to safely merge these technologies into your networks and workflows.

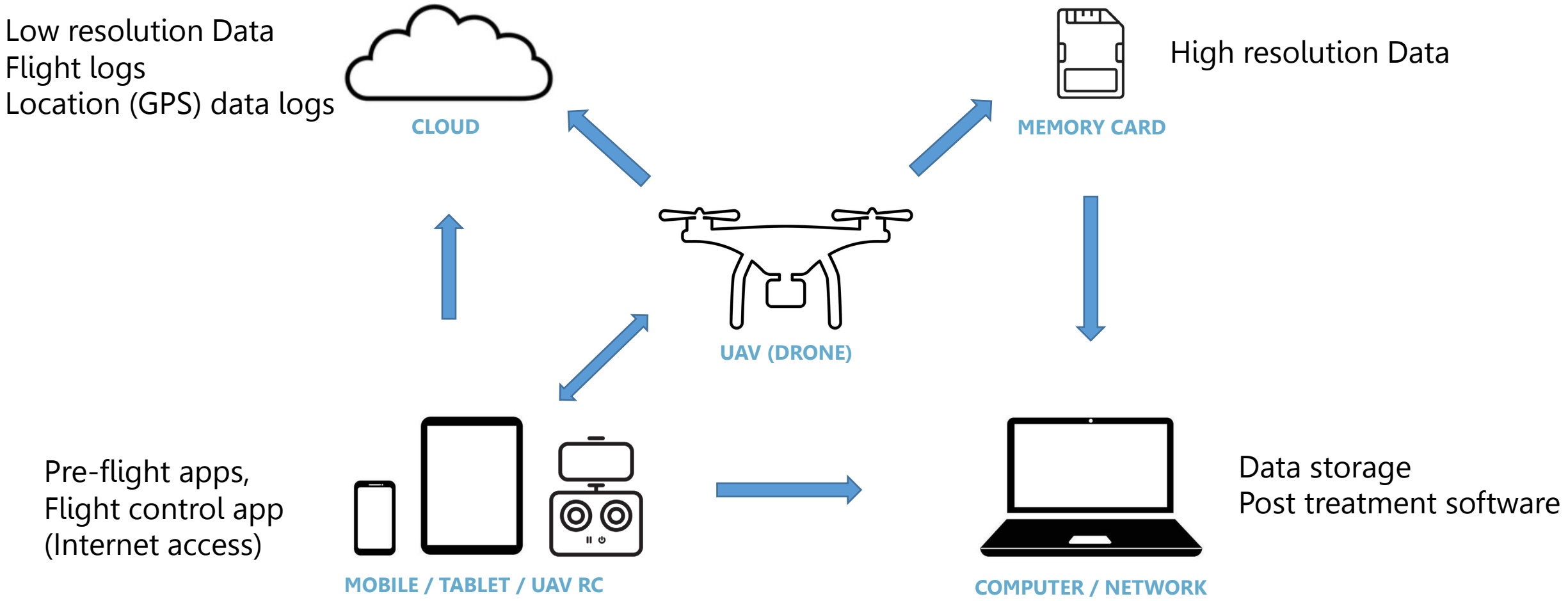
1- Security issues

2- Infrastructure challenges

3- The suspicion of foreign interference

ADDITIONAL CONSIDERATIONS (continued)

Relationship of data with software and hardware in UAV systems



ADDITIONAL CONSIDERATIONS (continued)

SECURITY ISSUES

1. The installation of external software connected to the internet in employees' computers and/or mobile phones.
    - 1.1 App for flight control application (usually on mobile or tablet)
    - 1.2 Apps for flight planning and preparation (weather, flight regulations)
    - 1.3 Apps and software for automated mission planning / data collection (Pix4D, Drone Deploy…)
    - 1.4 Memory cards for later data transfer
2. The physical connection of drones to computers/mobile phones and tablets (for updating of drones and related systems, …)
3. External data management in existing systems (hardware/software, photos/videos, live video streams, 3D point clouds, …)
4. The sharing of information with manufacturer and external drone services companies through cloud servers (data processing software, UAV fleet management software, logbook management)

To mitigate the risks, you have to either integrate all these parameters into your company’s existing security practices, or you can isolate dedicated hardware for drone operations (dedicated computers / mobiles / tablets, managed outside your network).

ADDITIONAL CONSIDERATIONS (continued)

INFRASTRUCTURE CHALLENGES

1. Are your existing systems ready for software that eventually requires computing power (like 2D and 3D photogrammetry, UHD Video, 3D point clouds, ...)

    1.1 Sufficient storage space; (4K/60 = 750 mb/min, 1080p/60 = 350mb/min)

2. Integration of external software into existing servers (ex: Pix4d, Drone Deploy, ...)

3. Integration of real-time data into existing systems via VPN, RTMP and live streaming system (video streams, ...)

4. Internal cloud interconnectivity and software related to drones (via APIs)

ADDITIONAL CONSIDERATIONS (continued)

THE SUSPICION OF FOREIGN INTERFERENCE (DATA LEAKS)

1. Current state of specific manufacturer bans in the U.S.

2. Impact of these bans on the industry (alternatives)