Submission 151 - Mirragin

COMMERCIAL-IN-CONFIDENCE

MIRRAGIN

CONSULTING | DRONES | ROBOTICS | AI

REMOTE IDENTIFICATION SUBMISSION

Mirragin Remote ID Submission
//
BRIEF
July 2023

Contact Details:
Josh Bailey
Counter and UAS Specialist
[redacted]
Email josh.bailey@mirragin.com.au

TABLE OF CONTENTS

OUR TEAM

Firstly, we appreciate the opportunity to provide advice on such an important step for the UAS industry. As an Australian SME with specialist UAS experience across many levels of Government, Defence, Airspace, law enforcement and emergency services, Mirragin have a responsibility to assist with the development of UAS policy as the industry grows and matures.

Our team consist of several specialists that have worked on development of the National Drone Detection Network (NDDN), Flight Information Management System (FIMS), and the Defence Counter-UAS. Therefore, our submission focuses heavily on this experience with an eye toward the future of airspace management.

DATA AND ACCESS

This is an ever-growing area of concern across the globe, and there is an important balance to be achieved with regard to the data that is collected, stored and made accessible to people other than the 'owner' of that data.

1. Who should have access to Remote ID data and to what information?

a. Firstly it's assumed there will be a wide range of stakeholders that will access Remote ID information such as:

    i. Other airspace users;

        1. UAS operators (commercial / recreational)

        2. Crewed aircraft operators – if the intent is to increase public safety and situational awareness for all airspace users, then it is important that equivalent requirements are placed upon 'manned' aircraft operators to both monitor and broadcast their position data to the same standard as UAS.

        3. Air Traffic Control / ATM/UTM systems – This may only be applicable for specific UAS activities within controlled airspace.

b. Then, in addition to the airspace users, there will be several stakeholders that will have an interest in the data that is being generated or managed such as:

    i. Defence,
    ii. Law enforcement,
    iii. Air Services / CASA,

iv. Other Government departments,
v. Other commercial operations (ie those that may not use airspace but will be affected by airspace usage).

c. Therefore, it is critical that each user or interested party is managed with 'permissions', and this would be a significant project to investigate, analyse and deliver a plan.

d. As a general rule, we would recommend a minimum level of information provided to people that don't have a 'Need to know'. This can be achieved through a login system with allocated permission levels of information access, for example:

i. Lowest level of access = General (Non-aircraft or UAS operator) Public
    1. Remote ID number
    2. Authorisation status (is it flying under a CASA or Auth approval?)
    3. Is it flying in accordance with the law? (may help to reduce complaints and unintended

ii. People Flying/Operating aircraft/UAS
    1. Enough information for safety (i.e. drone location, heading, altitude, speed)
    2. Remote ID for logging if required

iii. Law Enforcement
    1. Requirements for information are most likely related to preventing or enforcing public (safety), security and privacy concerns.
    2. Law enforcement should be restricted from viewing data without specific warrants or approval process.

iv. Defence / Government
    1. Requirements for information are most likely related to preventing or enforcing airspace (safety) and security concerns.

2. Should there be a data collection standard?

a. Yes, there should be a standard, to ensure clarity with industry, users and other parties with vested interests. Also, there have been a number of criticisms raised of the FAA's Remote ID approach, mostly relating to a lack of clarity in the information published, and therefore Australia would benefit from learning those lessons prior to delivering an equivalent system.

b. A data collection standard will also assist with the development of Remote ID 'beacons' that would be retrofitted to units that are manufactured without or prior to integrated Remote ID.

c. A standard also allows Australia to align to similar countries, which reduces barriers to commercial businesses that may need to travel between countries, IF a standardised set of rules can be maintained.

3. What is the best method of providing Remote ID data to relevant stakeholders?

a. A general principle, the minimum data should be given to people with the right level of access to achieve a task within a timeframe.

b. Using the FAA as an example, their Remote ID details the following data to be collected:
    1. Remote ID number
    2. Drone coordinates (GNSS)
    3. Height Above Takeoff (ATO)
    4. Altitude
    5. Speed
    6. Direction
    7. Pilot Remote ID
    8. Pilot Coordinates (GNSS)

c. In videos demonstrating the Remote ID transmitted from a DJI drone, it appears that remote ID beacons transmit all the above data without encryption and is freely available for anyone with a receiver or mobile phone app. This is a serious data privacy issue and may breach the Communications Act in Australia.

d. The two methods that CASA have mentioned seem to be fit for purpose; however, the FAA model for **BRID** will mean that anyone with a 2.4GhZ receiver can see the users information. This is not generally fit for purpose, and opens drone operators up to potential vigilantism, theft, or a myriad of other nefarious or disgruntled actors. Therefore, there needs to be a 'User Login' type system that requires identification of some sort, and rather than a completely open transmission it should be encrypted.

e. On the other hand **NRID** seems much more useful for some other user groups, so should be considered as an option for implementation, noting that the FAA have not used this method initially, it seems a much more infrastructure intensive activity, and therefore take longer to implement. Further analysis is given below on NRID.

f. Nefarious use of Remote ID Data should be assumed as likely, and the system needs to be secure enough that provision of data never results in a user's data being used or promulgated without their consent.

g. We also recommend facilitated working groups to test the access/data levels, including a 'red team' to test against nefarious actors accessing data.

4. What types of drone operators should be required to carry Remote ID equipment to operate drones?

a. Those operators that are flying within any airspace that CASA currently require drone operators to seek permission (from CASA or ATC) or require someone with a REPL to operate within.

b. We believe that any requirements should consider the following factors to require Remote ID:

i. **Airspace –** As per current regulations, operations within controlled airspace etc.

ii. **Size (MTOW):**
    1. **<250g** – Required only in specific airspace.
    2. **<2kg –** Required only in specific airspace.
    3. **>2kg** – Required unless in a FRIA (or equivalent)

iii. **Type of operations:**
    1. **Indoor or 'sheltered' –** Not required.
    2. **Tethered –** Not required unless in specific airspace.
    3. **Other limited or mitigated operations,**

5. How can Remote ID privacy issues be managed?

a. Security framework:
    i. Put in place several layers of security to ensure data is only collected by authorised personnel, under approved conditions.
        1. Only registered operators should be able to see certain types data
        2. Law enforcement require approvals similar to current process of warrants/judge approvals etc.
        3. Government require approvals under specific circumstances, for limited time windows.
        4. Encryption standard for data TX (especially BRID)
        5. User level hierarchy, with all users of an 'app' required to provide verified user profile (to dissuade potential bad actors)

b. Technological limitations:

    i. Broadcast of a Remote ID is limited to:

        1. Only functioning when aircraft is in operation (take-off).

        2. Only those with the right equipment (certified or according to a standard), registered with a login and identification linked.

TECHNOLOGY

1. Is Remote ID (BRID, NRID or both) an appropriate solution for Australia?

a. A combination of BRID and NRID dependent on operator and drone categories would seem the best solution, as it allows the mitigation of several risks that currently limit the grreater objective of Air Traffic Management (ATM).

b. BRID – Broadcast Remote ID - Transmits locally via Bluetooth/WiFi (2.4/5.8ghz)

i. Risks:
    1. Range can be limited to VLOS and may be an issue in areas with high interference or obstacles (ie. Cities)

2. Less secure data (anyone with a receiver can see data)
3. If there is a need to use the data for airspace deconfliction, there will be a need for a significant infrastructure network of BRID receivers/bearers to detect broadcasts and transmit the data back to storage / analysis locations.

ii. Benefits:
1. Security: If data is not stored locally or captured from a receiver, then it effectively disappears and there are no ongoing security risks
2. It is possible to limit who can see the Broadcast Data (ie encrypt the data packets, so only those with registered receivers can decrypt the data)

c. NRID – Network Remote ID - Transmits using Cellular data (LTE,4G/5G/XG)

i. Risks:
1. Data collection, storage, security
2. Potential for misuse of data by Govt bodies or Law enforcement
3. Operators in locations where there is no cellular signal will be restricted, and this is a potentially large issue for sectors like agriculture, mining as well as emergency services or Defence that often operate in remote areas.
4. Possibly restricts the types of UAS that can be used if they don't have the ability to connect cellular device / transmission link.

ii. Benefits:
1. More secure data compared with BRID, as it is easier to limit access to data
2. There may be less/no requirement for additional hardware if used with mobile app

2. Are different types of Remote ID more fit-for-purpose in different contexts or applications?

a. BRID
i. More suited to smaller / recreational drones
ii. More suitable for regional/remote areas (no cellular network coverage)

b. NRID
i. More suited to cities/urban areas (higher interference)
ii. More suitable for commercial operations
iii. More suitable for BVLOS

c. Note: these types of Remote ID will be extremely difficult for any nano sized drones to comply with due to size/weight therefore recommend they are excluded from this ruling by size and weight.

3. Are there other types (or variations of types) of Remote ID that should be considered?

a. **Hybrid** – this may require more complex Remote ID setups, but the combination of a BRID/NRID with dual transmission would potentially mitigate the risks of both systems, however, would be more important for

4. What factors should Remote ID mandates be based on, e.g. location, airspace related, other?

a. **Location** – There may be a benefit to delineation of urban areas (ie high-traffic, densely populated areas), as well as remote areas. This would be separate to airspace mandates, as there will be different types of airspace within an Urban area, for example.

b. **Operation type** - Commercial, recreational, sheltered, below X foot (AGL) ceiling,

c. **Airspace** – As per current airspace restrictions, however, would recommend adding similar to US FRIA sheltered/contained operations (ie contained within

5. What technical requirements, standards and governance arrangements should be considered in the introduction of Remote ID to position for integration with adjacent systems, including the development of the UTM ecosystem?

a. In the USA they have a standard for remote ID and tracking – F3411-22A, this should be considered to ensure we are aligned as much as possible for international integration of UAS operations in the future.

b. As per the above recommendations for Data Management – we recommend data being limited by user levels (and permissions), security and also separate databases that will need to be agreed to by a user prior to seeing or sending information.

6. What features does Remote ID require to ensure tamper resistance and to mitigate security issues (including cyber risks)?

a. Physical tampering may require disincentives such as regulations to fine those tampering with systems.

b. Software or electronic tampering may require data security standards, and user access control as per above.

USAGE

1. What impacts could mandatory equipage have on drone operators?

a. **Cost prohibitive** – drone adoption is currently high because costs are relatively low, therefore any regulation that adds cost will increase barriers to adoption. This should be carefully considered and could affect the wider industry, as most that work in the UAS industry began as recreational operators.

b. **Weight** – Flight time is reduced, momentum and kinetic energy are increased, therefore this may push operators over MTOW limits if the system is large or heavy, and thus cost more.

c. **Knowledge required to install and operate** – this is a significant barrier to adoption.

d. **Broadcasting controller and drone location** – As stated above, potential theft, interdiction, vigilantism and other nefarious actors can potentially see a UAS operator and their aircraft location.

2. Should mandatory equipage be rolled out to all drone operators, or phased through types of operators and/or operations?

a. Phased introduction is recommended to ensure that any 'issues' arising can be resolved at each phase. Start with smaller groups and move to larger groups.

3. Are there existing standards that should be considered/adopted to facilitate Remote ID uptake in Australia?

a. Yes - In the USA they have a standard for remote ID and tracking – F3411-22A this should be used as a guide but may require some updating for Australian specific purposes.

4. Who should we be engaging with, particularly outside of the aviation industry (e.g. telecommunications providers)?

a. In addition to the airspace users, there will be several stakeholders that will have an interest in the data that is being generated or managed such as:

i. Defence,
ii. Law enforcement,
iii. Air Services / CASA,
iv. Other Government departments,

v. Ports and Critical infrastructure,
vi. Other commercial operations (ie those that may not use airspace but will be affected by airspace usage).

We appreciate the opportunity to comment on the Department's initiative and are available any time to assist with the overall project. Please reach out and contact us any time if you have any points of clarification required.

MIRRAGIN
CONSULTING | DRONES | ROBOTICS | AI

Level 6,
200 Adelaide St
Brisbane Qld 4000

www.mirragin.com.au