Submission 130 – Swoop Aero

Swoop Aero Pty Ltd
ACN 20 624 870 775
Port Melbourne
Victoria 3207 Australia
www.swoop.aero

Department of Infrastructure, Transport,
Regional Development, Communications and the Arts
GPO Box 594
CANBERRA ACT 2601

27 July 2023

Subject: Swoop Aero submission to the Discussion Paper for Consultation on Remote Identification (Remote ID)

To whom it may concern,

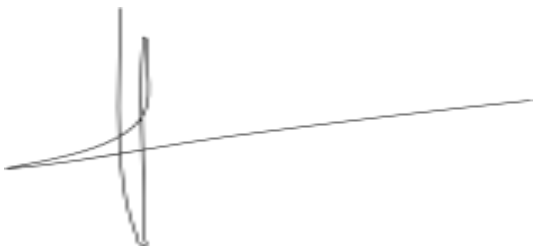
Swoop Aero welcomes the chance to provide feedback on the Remote ID Discussion Paper, and thanks the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRCA) for this new round of consultation.

As we operate both internationally and within Australia, we are committed to providing feedback, suggestions and recommendations to assist with the continuous evolution and improvement of drone regulations, incorporating significant operational experience.

We note and appreciate the changes that have been made to the Discussion Paper and we continue to support the introduction of Remote ID requirements in Australia.

Please see our submission attached to this letter.

Sincerely yours,



Kind Regards,

Marion Hiriart
Aviation Strategy and Government Relations Manager
Swoop Aero

Discussion Paper for Consultation on Remote Identification: Swoop Aero's submission

Swoop Aero views the development of recommendations to enhance the Australian drone regulatory regime and enable continued integration of drones into Australian airspace as both timely and necessary.

The exponential growth of the use of drones presents unique challenges and opportunities for regulators. Improving the current rule set will enhance aviation safety while also ensuring that Australia makes the most of the economic, social and employment opportunities that the continued growth of the sector presents.

Data and access questions

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

Remote ID data should be held by a Government entity, e.g. CASA and be accessible by other government entities on demand.

The information sent from the drone would assist CASA, law enforcement authorities and other security agencies in identifying a drone and locating its operator. This functionality is particularly important for drones that are breaching the rules in a given area, or those operating in restricted airspace near aerodromes and other sensitive facilities.

The general public could also access basic data to identify a drone in a way that would protect the privacy of the owner or operator's information. Remote ID would provide more transparency while still ensuring drone owners, pilots, businesses and customers' privacy.

The existing registration system would be the basis to provide the information necessary to identify drones and their owners when required (through a unique identification number). Remote ID requirements would thus build on this measure, and be implemented after the set up of the registration system, in adherence with Australian privacy legislation.

2. **Should there a data collection standard?**

See Question 1.

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

-

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

There should be a focus on aircraft conspicuousness, with all airspace users not equipped with EC devices like ADS-B included in the mandate. In other terms, all drones operators should be required to possess and use Remote ID equipment when operating, except:

- Operators using model aircraft (only when flown in danger areas);
- Operators using drones weighing 250g or less (for consistency with existing policies and regulations); and
- Operators equipped with existing aviation-approved surveillance systems (ADS-B or FLARM) with a higher level of integrity, providing Remote ID is interoperable.

In relation to airspace, drone operations are mainly taking place outside of controlled airspace (Class G). While ATC does not separate air traffic in Class G, traffic information is passed to the IFR aircraft. Network Remote ID would allow ATC to pass traffic to an IFR operation.

For separation in Class C and above, no separation standard exists in the Manual of Air Traffic Services V62.5 for a Remote ID position. Drones would need to provide a GPS position, which would place an undue burden on ATC as a procedural separation standard would need to apply.

To operate in Class C and above Airspace, Drones will require ADS-B or a Remote ID position to be accepted as a Surveillance track.

5. **How can Remote ID privacy issues be managed?**

Remote ID requirements will have to be developed with the following points in mind:

- Ensure current, and future privacy requirements for commercial drone operations remain proportionate and practical. While it is important to ensure that drone operators remain compliant with Privacy laws, it is also vital to ensure that the industry is not unduly burdened by unnecessarily strict requirements that would stifle its growth. Further limitations on operations must be justified, and any new measures must remain adequate to achieve the envisaged objective.

- Improve social licence and ensure public education. It is important to ensure continuous communication with the public on drone use and privacy and what can and cannot be done (e.g. what constitutes a breach, what is allowed, etc.). There is still a lot of misunderstanding from the public on Remote ID and, more generally, drone use. While we are spending a significant amount of time working on social licence through our operations, the Government's support is needed to prevent miscommunication and ensure the targeted education objectives are met.

Technology questions

6. **Is Remote ID (BRID, NRID or both) an appropriate solution for Australia? Is one type of Remote ID preferable over another? Are there other types (or variations of types) of Remote ID that should be considered?**

Remote ID could be a suitable and appropriate solution for Australia, provided it effectively solves the identified problems and achieves integration and other benefits.

At this stage, both types of Remote ID should be considered. Further work needs to be conducted on the possible implementation and the availability of the technology; this will help identify and assess the risks and impacts of any new requirements.

It is important that drone operators equipped with existing aviation-approved surveillance systems (ADS-B or FLARM) with a higher level of integrity should not require an NRID system but instead integrate existing flight information into the NRID Service provider.

Adopting a proportionate and risk-based approach with Remote ID will be necessary. It is important to ensure the interoperability of Remote ID with other electronic conspicuity (EC) devices and to promote fair expectations for drone operators. In other terms, to achieve safe integration, all operators must be electronically conspicuous - including those operating out of controlled airspace (Class G) - and share the same burden (costs) and reward (situational awareness).

Similarly, given the data messaging available with Remote ID as detailed in ASTM F3411-19 Section 5 and the relatively cheap cost of implementation, the use of Remote ID for other airspace users currently operating inconspicuously should be investigated.

Finally, it is important to acknowledge that the effectiveness of Remote ID would be limited for enforcement. It is improbable that nefarious operators comply with any Remote ID requirements when using drones and would likely find a way to circumvent it. This would result in additional costs for compliant users and would not necessarily help enforcement.

7. **What factors should Remote ID mandates be based on? E.g. location, airspace related, other?**

Since the main objective is safe integration through identification, the mandate should be as broad as possible. But it would eventually depend on the effectiveness and compatibility of the available standards and devices.

Please see below a non-exhaustive list of factors to be considered:

- Types of operators: there should be a focus on aircraft conspicuousness, with all airspace users not equipped with EC devices like ADS-B included in the mandate. In other terms, all drones operators should be required to possess and use Remote ID equipment when operating, except
    - Operators using model aircraft (only when flown in danger areas);

    - Operators using drones weighing 250g or less (for consistency with existing policies and regulations); and
    - Operators equipped with existing aviation-approved surveillance systems (ADS-B or FLARM) with a higher level of integrity, providing Remote ID is interoperable.
- Airspace: operators operating in special use airspace like danger areas - provided they stay within the said airspace - may not be required to use a Remote ID device since other airspace users must be aware of the area they are flying in through the use of NOTAMs. See FAA Advisory Circular 89-3 "FAA-Recognized Identification Areas" as a similar concept.
- Effectiveness and regulatory acceptance of Remote ID as a Tactical Mitigation Performance Requirement (TMPR) in the SORA.
- Availability of technology/devices: currently limited, given the novelty of the standards and technology.
- Complexity of the operations.
- Costs, e.g. retrofitting of existing aircraft, etc.

8. **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?**

The availability of standards that support new functionality, such as Remote ID, is currently limited. While standards have now been developed, there will need to be a level of flexibility in adopting commercial off-the-shelf products that fulfil the requirements and home-built options that may be more prevalent in the drone community.

For harmonisation's sake and as mentioned in the document,, the Australian government should consider standards like ASTM 3411 and ASD-STAN – prEN 4709-002 further.

In relation to UTM, it will be important to ensure that any form of UTM implemented post-adoption of Remote ID must be capable of ingesting data in the prescribed formats and not require any software or hardware changes.

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

We consider this point crucial, given the lack of a current Whole of Government approach to RPAS cybersecurity. Policies, regulations, and standards on cyber security should be a core part of the drone work programme. They will have to be investigated, developed and implemented simultaneously with the rest of the measures.

Additionally, many Original Equipment Manufacturers (OEM) are currently undergoing Type Certification, and the implementation of any cybersecurity requirements after that is complete will become exceptionally burdensome.

Remote ID requires the following features to tamper resistance and mitigate security issues:

- Physical Protection: Remote ID chips/hardware should be embedded within the airframe as part of the manufacturing process and should not be accessible to end users.

- Software Protection: the aircraft should complete a health check of the Remote ID system across all transmission methods (BL4/BL5/Wifi) and receive it via a completely separate chip, validating both inbound and outbound Remote ID are operating on all channels. If this check is failed, the drone should not be able to take off.

- A check to ensure the firmware onboard the individual Bluetooth chips should be completed before start-up to ensure someone has not attempted to tamper with the module's firmware.

- Suitable protection of the onboard logic to prevent any firmware not correctly certified by manufacturing from running onboard.

- The operating system should be protected to ensure no alterations can occur once loaded. Files that the operating system does need to edit, logs and configuration files should be stored entirely separately.

Usage questions

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

Remote ID would provide an increasingly important level of information and situational awareness to airspace users, other drone operators, and regulators as the frequency of operations increases. This is particularly important to Swoop Aero in terms of allowing safe and equitable access to all kinds of airspace.

However, this introduction must be considered part of a more holistic review of appropriate EC requirements for all airspace users. Currently, the onus is wholly on drone operators to avoid conventionally piloted aviation. However, in many circumstances, groups like General Aviation are not required to do anything except utilise see and avoid strategies through a limited field of view.

Mandatory equipage of EC (such as Remote ID) would help build increased trust and robustness in Remote ID, eventually allowing it to become a suitable tactical mitigation system for Air risk classes (ARC) -c and -d.

The main impacts on drone operators and manufacturers would be time and costs of compliance associated with any new requirements, the additional weight on the aircraft or any moves towards the certification of aircraft designs. These factors would dictate whether operators would comply with this requirement.

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

See Question 4.

It is important to keep in mind that many consumer drones are already equipped with Remote ID (hardware or software) or with other forms of EC.

With the Australian Government providing financial support for VFR operators to install ADS-B, the introduction of a Remote ID mandate should coincide with an ADS-B mandate for VFR aircraft. With drones broadcasting their position, rules of the air, including the right of way, should be reconsidered, i.e. drones equipped with EC devices or Remote ID should have priority over crewed aircraft that are not equipped with ADS-B or other forms of EC.

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

See Question 8.