Submission 146 – Wing Aviation Pty Ltd

Wing

Submission from Wing Aviation Pty Ltd
Discussion Paper on Remote Identification (Remote ID)

Wing welcomes the opportunity to respond to the Department's discussion paper for public consultation on Remote ID. This technology can serve as a critical tool to facilitate valuable data exchanges between individual uncrewed aerial systems (UAS) entities. Through Network-Based Remote Identification (NRID), government agencies and other users also can have enhanced and secure visibility into this digital identification data.

Any policy the Department adopts regarding Remote ID should support the development of UAS Traffic Management (UTM) and Beyond Visual Line of Sight Operations (BVLOS) operations. To foster the certainty and consistency that is needed for the UAS industry to operate at scale, Wing agrees with the Department that global harmonisation and industry collaboration will be essential. As such, the Department would benefit from aligning their regulatory framework with other international standards, such as ASTM F3411-22a, which reflect established industry consensus of performance requirements that are reasonable for both commercial operators and hobbyists. Deviation from such existing standards, which encompass a diverse range of operating environments, could cause fragmentation and hinder growth in the UAS industry.

Given the diversity of operators and operating environments within the UAS industry, Remote ID requirements should be performance-based and may be determined by the airspace and type of operation. The Department should allow operators to choose the Remote ID technology that is best suited for their particular operating environment, subject to meeting performance requirements. If operators meet the required level of performance, they may be exempt from redundant or unnecessary Remote ID requirements. Mandating the usage of Remote ID equipment for hobbyists, with more limited CONOPS than commercial drones, would not be proportionate to the scope of hobbyist operations and would be detrimental to the hobbyist community.

While the Department should empower operators to choose between NRID or Broadcast Only Remote Identification (BRID), Wing believes that NRID is better positioned to serve as the industry standard in areas with internet connectivity, though persistent connectivity is not required for the successful functioning of NRID. Wing disagrees with the Department in its characterization of cybersecurity as an advantage for BRID and a challenge for NRID. BRID presents risk for unrestricted data collection or aggregation of Bluetooth and Wi-Fi data. As the Department notes in this paper, "data compromise risk may still exist as anyone with a suitable receiver could potentially obtain data through BRID." NRID's technology protects against the aggregation and exploitation of sensitive data for consumers and businesses, and it allows for increased but tailored access to Remote ID data for other users and agencies, while still maintaining the needed level of privacy. Per ASTM F3411-22a, data at rest, as well as communications facilitating the transit of data, will be encrypted using an industry-standard encryption mechanism with a minimum encryption strength of 128 bits. In light of these many advantages, Wing agrees with the Department in referring to BRID as "limited" and NRID as "standard."

Thank you for your continued efforts to solicit feedback from stakeholders both inside and outside of the aviation industry on this important topic. We appreciate and recognise the updated draft paper's reflection of some of these recommendations, including distinguishing Remote ID technology from Detect and Avoid (DAA) capabilities. Wing is confident that the Department can develop Remote ID rules that are performance-based, tailored to the airspace and type of operation, and empower operators to choose the best Remote ID technology for their operating environment.

Department's Individual Questions:

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

There should be widespread access to Remote ID data, not only for UAS operators but also government entities and the general public. Everyone should be able to see all UAS operations within the area they select, and the required fields in ASTM 3411-22a should be accessible to all.

Through standard Remote ID, detailed information may be available for authorised government users.

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

Wing incorporates both country-specific and global data collection standards in the design and building of its services and operations. As such, we abide by Australian privacy principles and standards, as well as the GDPR.

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

The UAS industry is best suited to provide solutions that meet the needs of diverse operational requirements for safe and efficient uncrewed operations. As with UAS operators, requirements for service providers sharing Remote ID data should be performance-based. Any time Remote ID data is accessed or exchanged, it is of paramount importance to adhere to data privacy safeguards. In cases where Remote ID information is shared between providers, a peer-to-peer scheme will lessen the ability for a central point of failure. Using NRID, communications between UAS operators, as well as communications between UAS operators and service providers, have the added mitigation of encryption.

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

If drone operators can achieve the required level of performance, they should not be required to carry Remote ID equipment. This may be achieved through compliance with standard Remote ID means or through the ASTM F3411 'area-based' declaration.

UAS with an operating weight of less than 250g may be considered for exemption from Remote ID requirements due to their significantly low profile. UAS operating under IFR should also be excluded from consideration given their different form of communication with the airspace system.

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

Given BRID's risks of aggregating and potentially exploiting personal information, the Department should not mandate the usage of BRID and instead permit operators to choose the Remote ID technology that is best suited to their operating environment. Through regularly disposing of data that is no longer needed and tailoring access to data to various stakeholders, NRID is better equipped to protect privacy and sensitive data from operators and customers. ASTM F3411-22a also reinforces the concept of preserving privacy by only sharing needed data and discouraging Remote ID as a means to perform ongoing surveillance.

Australian Remote ID requirements should also impose limitations on data viewability and retention between Remote ID providers to prevent the unrestricted collection or aggregation of network data by a third party Remote ID USS or Remote ID USS user. The ASTM standard provides examples of effective restrictions, including limiting the viewable area (2km for aircraft-specific information, or 7km for a depiction of generalized aircraft activity) and requiring the disposal of shared data (after 86,400 seconds, or one day).

6. **Is Remote ID (BRID, NRID or both) an appropriate solution for Australia? Are different types of Remote ID more fit-for-purpose in different contexts or applications? Are there other types (or variations of types) of Remote ID that should be considered?**

Remote ID policies that support BVLOS operations and empower industry-led UTM will be an invaluable tool in Australia and globally. The Department should empower operators to choose between NRID or BRID upon assessing which technology would be better suited for their operating environment as long as they successfully meet the performance requirements.

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

If the Department pursues any mandates for Remote ID, they should be scoped in such a way that is tailored to the airspace and type of operation. For instance, the hobbyist community has a reduced scope and complexity of operations compared to commercial drones, so hobbyists have less need to rely on complex requirements. However, the UAS industry as a whole, including commercial drones and hobbyists, would likely not encounter difficulties in complying with Remote ID requirements comparable to ASTM F3411-22a.

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 Department should utilize ASTM F3411-22a, which reflects established industry consensus, as the standard for Remote ID performance requirements for both commercial drones and hobbyists. Usage of this standard would support global regulatory harmonisation for the UAS industry. While CASA will select Remote ID performance-based rules and oversee the entry of participants into the UAS ecosystem, industry will be best suited to find solutions to develop and maintain a UTM system.

There is on-going work aimed to establish a governance structure that can be harmonised globally. In Switzerland, under SUSI, industry executed the first Master Agreement which established rules for data-sharing between Remote ID providers. In the United States, the FAA just completed their UTM Field Test which will deliver recommendations for service provider governance when sharing UAS information. It is also expected that an effort will be kicked off shortly to develop a global USSP-USSP data-sharing agreement as required by the European Union's U-space regulatory package. The Australian government should look to participate in these conversations and help to shape a governance agreement that can be harmonised with other UTM environments.

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

As with other facets of Remote ID, tamper resistance requirements should be performance-based to ensure that others are unable to interfere with Remote ID's successful functioning. The FAA has incorporated this approach in its Remote ID Rule by requiring UAS with Remote ID to be designed and produced with functional tamper resistance protection to prevent unauthorized changes to the Remote ID equipment or messages. The encryption capabilities in NRID provide protections for communications between UAS operators, as well as between UAS operators and service providers.

Though Remote ID serves as an invaluable security tool in the UAS ecosystem, it is important to have a full understanding of the relative risk that this technology proposes. With all of the protections built into NRID, it is extremely unlikely that any information being exchanged would be compromised. However, in an unrealistic hypothetical in which such a breach transpired, it would not result in a major threat to surrounding aviators, particularly given that this information is not safety critical, as well as the fact that the UAS would not be transporting any people.

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

One of the most immediate impacts of mandatory equipage of Remote ID for operators would be size, weight, and power bargains, as well as the time and cost associated with compliance. These requirements could potentially require equipment that is incompatible with certain aircraft and force operators into limited hardware options. If operators are required to use BRID, the UAS industry could have weakened privacy protections and experience increased risk of the capture and aggregation of BRID data. Mandating equipage instead of focusing on achieving performance outcomes for Remote ID would be particularly difficult and affect the future scalability for smaller commercial operators and hobbyists.

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

Rather than mandating equipage for all operators, the Department should follow a performance-based approach. Any Remote ID policy should consider factors such as airspace and type of operation, including distinguishing between hobbyists and commercial drone operators.

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

To aid global regulatory harmonisation and adhere to established industry consensus, the Department should adopt ASTM F3411-22a.

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

The Department would benefit from engaging with stakeholders both inside and outside of the aviation industry. Within the industry, the Department should collaborate with the spectrum of UAS participants, including commercial operators, hobbyists, service providers, manufacturers, and industry groups such as the Australian Association for Uncrewed Systems (AAUS). To progress global harmonisation of UAS regulations, the Department should coordinate with other international regulators overseeing the UAS industry.

The Department also should engage with non-aviation entities, including Australian communities and local governments, to hear their unique perspectives and further societal awareness of the potential benefits and diverse use cases of drones. Given that the degree of importance for telecommunications providers varies by operator and service provider, engagement with this sector is not as critical as the above entities, which will be directly involved in the UAS industry.