Remote Identification Discussion Paper Response

[redacted]

June 22, 2023

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

Only CASA and authorities should have access to full data, that is the RID protocol should only broadcast privacy insensitive data such as the operator/aircraft identifier and flight parameters. Broadcasting private information would put end users at risk regardless of encryption mechanisms used.

2. Should there be a data collection standard?

Yes, rules and penalties for all bodies dealing with RID data need to exist to help prevent leaking of private information.

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

NRID data should be aggregated at the network layer to provide a real time picture of all RID equipped aircraft, stakeholders take on the task of collecting and storing flight parameters in their own IT infrastructure. That is the RID network should be an ephemeral event relay system to minimise complexity and provide always up to date data to those interested.

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

All commercial or for profit operators where the gross weight of the aircraft exceeds 2kg. Recreational users should be exempt as the vast majority operate either sub 250g aircraft (toys or micro drones intended for indoor use where zero risk of injury or damage to property exists) and those building or buying larger FPV drones or fixed wing aircraft for fun.

While these larger aircraft, particularly drones, have a theoretical risk to the public in terms of injury or nefarious use (use as a kinetic weapon, drug smuggling into prisons, observation of security sensitive installations), the entry cost (both monetary and time investment in skill needed) is at such a level that the users of these aircraft take on the responsibility fully to ensure that no harm comes to the public. The concept that RID will somehow prevent or discourage criminal use is completely unfounded and will only serve to bolster the level of sophistication used in any of these dreamt up attacks.

Additionally rural operators of large >2kg aircraft for the purposes of primary production should also be exempt as the airspace they operate in is already uncontrolled and no risks to people or property would be mitigated by RID, existing laws and the high cost of these aircraft provide enough incentive to prevent stunting or other irresponsible use.

5. How can Remote ID privacy issues be managed?

All personal information must be kept by one central body (CASA) and can only be requested by authorities where an active investigation is taking place. Allowing public or 3rd parties free access to private information will lead to leaks, misuse and in some cases assault or other criminal offences against the aircraft owner by misinformed/unstable members of the public.

6. Is Remote ID (BRID, NRID or both) an appropriate solution for Australia? Are different typesof 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?

NRID should be considered as the only viable means within Australia, BRID is only applicable to recreational users of which there is little to no benefit in tracking. While BRID is cheaper in it's implementation, requiring only software and servers to handle the data it is simply not fit for purpose when dealing with coordination or airspace deconfliction.

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

RID should primarily be based on airspace, areas with high commercial drone use would benefit from automatic coordination through real time location data.

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?

As stated above the system should be an ephemeral event based system, the system should be built in a distributed fashion, that is processing nodes are strategically positioned both physically and in terms of network latency, nearest to areas of interest. These nodes can then by queried by the aircraft themselves only seeing information applicable to their current position. Each node would also send aggregate packets to nearby and centralised collection endpoints to build up a full picture of the airspace.

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

The best approach to security is an open approach. If the system is implemented in a way that requires operators to send sensitive information then rouge operators WILL falsify that information for personal gain. Anyone with a phone can fake their GPS location, anyone with a SDR and a little bit of reading can jam or degrade GPS systems over a large area, anyone who really wants to is going to find a way around whatever temper resistance is used on these RID modules and try to cause havoc. Attempting to secure the system at the edge is a waste of time and will lead to additional costs. Energy is better spent implementing detection of rouge operators on the server side, checking for RID duplication or coordinating efforts with the ACMA to detect jamming and other forms of espionage.

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

For commercial operators it will mostly be complaining about addition costs added. If RID is mandated for recreational users it will create a new black market for falsified RID modules, increase the number of stealth or high risk uses of UAVs such as night flying or stunting, and waste authority and CASA resources on false or uninformed reports from the general public. Furthermore, basically all recreational users operate within VLOS and below the tree canopy, tracking these movements has no practical bearing on commercial operators or aircraft in the area, those who fly BLVOS illegally or in conflicted airspace will not equip RID regardless of the mandate.

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

Phased introduction is needed to deal with the non-existent infrastructure, for example the Logan, QLD test site for drone deliveries would be a sensible candidate for mandatory RID usage as it allows for understanding the exact requirements needed for the system to operate in a high traffic environment, trying to enforce adoption everywhere before infrastructure exists will only lead to non-compliance and compromises in the way the system is implemented.

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

From a technical aspect a message bus signally system should be used at the edge, this will massively simplify implementation and allow for future scaling. There are many new technologies to pick from that would seem to fit the problem at hand but I think using a well proven and simple means of signalling is the way forward.

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

Me lol. Engagement with ISPs will be necessary to arrange dedicated bandwidth for exchanging data throughout the network, IT consultants from the private sector need to be approached for designing the infrastructure that will eventually deal with millions of UAVs at a time, this is a modern problem that requires a very carefully designed solution or it's simply not going to work. Particularly the real time aspect needs a lot of consideration to get right.