Submission 153 - DJI

DJI Response to the Department of Infrastructure's Consultation Paper on Remote ID

31/07/2023

DJI is the world's largest manufacturer of civilian drones. As the market leader, DJI has been vocal in supporting Remote Identification (RID) to create greater accountability among drone operators and to make the enforcement of existing drone rules easier. We have implemented Broadcast RID in Japan and the United States across all of our currently sold products as well as some of our older platforms.

As such, we would be in a position to implement Broadcast RID across the vast majority of the currently used drones in Australia should a broadcast standard based on ASTM F3411 be adopted. Depending on estimates used for market share, this would rapidly bring between 60-80% of Australian drones into compliance.

DJI so strongly believes in the benefits of Remote ID that we launched AeroScope in 2018. This was years ahead of regulatory requirements for Remote ID being present in any country. AeroScope provides RID for all DJI products and the RID information is visible to anyone owning an AeroScope unit.

Our Elevating Safety report, issued in May, 2019, called for all governments to require RID.

In addition, DJI played an active role in the ASTM International standards organization working groups that led to ASTM Standard F3411 for RID and the Means of Compliance F3586 accepted by the FAA. DJI was also the first company to have Declarations of Compliance accepted by the FAA.

In Australia, DJI held demonstrations of Broadcast Remote ID in Australia (Brisbane) several years ago to aid understanding of the benefits of broadcast RID and the ease with which it can be accomplished.

DJI's experience working on this issue since 2016, give us insights that we would like to share:

1) There is a strong body of work to pull from: the FAA's Remote ID Advisory and Rulemaking Committee issued its report in December, 2017. It took another four years for a rule to be promulgated. In that time, the ASTM working group spent close to two years working on the standard and an additional 18 months working on the Means of Compliance.

2) There is wide agreement on the preferred standard and format: FAA, EASA and Japan's MLIT have all mandated Wi-Fi Broadcast RID. This has been adopted due to ease of adoption and low cost of the solution. The EASA requirement of network RID for drones operating in U-Space cannot be said to be truly in effect due to the slow rollout of UTM and the complications involved.

3) RID has been rejected as a means of Detect-and-Avoid (DAA): FAA and others have looked at RID as a means of DAA and rejected it as a solution for DAA due to the increased complexity and higher standards for latency and other issues that would be required. In all jurisdictions with RID currently in place, the objective of RID is clearly for accountability, enforcement and security purposes. There is excellent work being done on the issue of DAA (such as ACAS Xu), but this is a separate issue and should not be combined with RID.

4) Broadcast Remote ID has been proven to be perfectly compatible with a UTM environment: In November 2018, DJI together with its partner Altitude Angel, demonstrated how Broadcast Remote ID can be integrated into UTM and ATM systems in order to manage traffic at and around busy Manchester airport in the United Kingdom. The trial, called Project Zenith, was a success and showed that all that's needed to bring Broadcast Remote ID into a UTM and ATM environment is to network the receiver, not the drone itself.

5) Broadcast Remote ID is ready right now: An added benefit would also be that major manufacturers already have to have Broadcast RID in place as it is required for any products sold in America after September, 2022. This means the rollout of firmware updates for most manufacturers should be quick and at no additional cost to the customer or manufacturer.

6) Broadcast Remote ID already exists in Australia: Every airport, national security site, police department or other entity deploying DJI's AeroScope units to pick up and read the signal broadcast by DJI drones is daily proof that Broadcast RID works.

Given the above, DJI believes the Australian government can quickly adopt Broadcast Remote ID using ASTM F3411. This would align Australia with other major regulatory jurisdictions and avoid spending years reinventing the wheel.

It is worth noting that ASTM F3411 allows for broadcast, network or Bluetooth for RID. If Australia wants to enable that level of flexibility in complying with a RID requirement, this would allow each manufacturer or even operator to decide on which solution to use. DJI only argues that broadcast should be among those options available to meet the requirement and warns that there will be additional problem solving and costs required to make Network or Bluetooth RID a reality.

We address the questions posed in the consultation document below.

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

We believe that the drone user identity should be easily viewable by law enforcement, aviation safety authorities and other government officials with security or enforcement needs. The display of information to the general public should show the serial number of a drone along with make and model. This is similar to a member of the public seeing a car license plate of an offender and reporting it to the police. The same concept should hold for RID. The member of the public would not be able to access personal identification information on the individual flying – this would be done by the police or other officials by matching to the CASA registration database.

Another issue is operator position or home point of the drone. This is required to be displayed by the FAA. However, this does raise concerns about members of the public taking matters in to their own hands if they can see where the operator is standing. If operator position is a required field, it will be difficult to protect that information from the general public as the signal needs to be readable if the above license plate effect is to be achieved. Doing away with operator position would hamper law enforcement. So, there are clear pros and cons to either course. One means of dealing with the issue might be a requirement for app developers of publicly available apps for reading RID to not display operator position

2. Should there be a data collection standard?

If the process above is followed, then PII should be protected and the only issue with data collection would reside with the CASA registration process.

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

Broadcast RID allows a simple smart phone to act as a receiving station. Therefore, an app would be the best means for enabling this for the general public and a separate app for government users could also access the CASA registration system to enable access to personal ID of the drone user. We expect that fixed installations such as airports or security areas would have antennae similar to a stationary AeroScope that enables longer range and a more holistic view of the airspace.

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

If Broadcast is an option, all drones with a certain threshold of capability should be included except those who fly at aeromodelling clubs. Aeromodelling clubs should be excluded as their members fly at designated sites and these clubs have a strong record of self-policing. In addition, many aeromodellers at these clubs fly numerous different self-built products and this would entail significant costs if they all needed a module for broadcasting RID.

If Broadcast is not an option, there should be serious thought to costs associated and what types of users need RID. Network RID would almost certainly require a much larger outlay of government expenditure on the infrastructure needed. DJI would oppose any attempt to pass on such costs to users as we do not believe a Network RID system is necessary for the accountability and enforcement role for which RID was developed. A separate modelling of costs followed by a consultation on those costs should be undertaken if Network RID is chosen as a preferred method.

If Broadcast is chosen, then defining the capability threshold of drones included in Broadcast RID should be done to weed out toy drones, etc that should not be the focus of RID. The FAA's 2017 UAS Aviation Rulemaking Committee on Remote Identification and Tracking ("2017 ARC") had a working group of air traffic, law enforcement, and national security members that considered the question of what UAS should be required to perform Remote ID, and concluded that UAS with either of the following characteristics should comply with remote ID and tracking requirements:

1. Ability of the aircraft to navigate between more than one point without direct and active control of the pilot.

2. Range from control station greater than 400' and real-time remotely viewable sensor.

See 2017 ARC Report page 29.

Drones that cannot fly further than 400' should not be the focus of RID regulations and the owner/operator should be easy to locate for this category of "toy" drones due to their limited range.

5. How can Remote ID privacy issues be managed?

A simple fix to keeping PII confidential and only viewable by law enforcement has been described above in the answer to Q1. In effect, the public should be able to view all the data transmitted by the drone. But the only ones with access to the matching registration records showing PII should be government officials with enforcement or security needs.

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?

Broadcast Remote ID is appropriate. The Federal Aviation Administration in the United States, European Union Aviation Safety Agency in the EU, and the Ministry of Land, Infrastructure, Transport and Tourism in Japan all have Remote ID rules already in place. In each case they have adopted the Broadcast Wi-Fi variant as the least expensive and burdensome option. In addition, Remote ID was discussed as a possible means of Detect-and-Avoid (DAA) by the FAA. This was rejected as the standard needed to meet DAA requirements was too high and the problems to be solved were too complex. Instead, the objective of Remote ID in each of the above jurisdictions is to increase accountability of drone operators, enable the enforcement of existing laws and regulations, and increased security. Broadcast RID achieves these ends and is proven to work. Network RID will entail significant costs and has not been proven to work at scale and suffers from issues of limited coverage in Australia. The FAA speculated that costs for a network remote ID system could be USD 582 million. DJI commissioned an economic analysis

by Dr. Christian Dippon of NERA Economic Consulting that put the total costs at more like USD 5.6 billion over a decade.

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

If Broadcast Wi-Fi RID is adopted and the objective is accountability, enforcement and security, there is very little reason to limit by location. The reasons are: A) the costs of the majority of drones being made Broadcast Wi-Fi RID compliant should be zero for the vast majority of drone users as this can be accomplished via a firmware update for most drones that use Wi-Fi signals for command and control links. The remainder should be able to meet the requirement with a small transponder. B) if the purpose is accountability and enforcement of rules, then there should be almost no limits on where this is applied.

The one area where RID would offer limited benefits is at aeromodelling club sites. Given that aeromodelling clubs are already self-policing effectively and have done so for decades, it would make little sense in forcing a user who only flies at club facilities to adopt a RID solution. Operators at aeromodelling clubs are also much more likely to operate kit-built drones without an easy RID solution other than attaching a broadcast module.

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?

ASTM F3411. This standard has formed the basis for rulemaking in the US, Japan and EU (the ASD-STAN standard is essentially very similar to ASTM F3411). If Australia wants to align and to grab low hanging fruit and avoid over complicating RID for manufacturers, users, and its own regulatory and policymaking bodies, it should adopt this standard. The hard work put into this over the past 4 years should not be duplicated. In addition, any manufacturer selling drones in the US past September 2022, would already have a solution in place to meet the US requirement. This means that the rollout for Australia should be simple for the vast majority of manufacturers if the Broadcast variant is adopted.

Integration of Broadcast Wi-Fi RID into a wider system for airspace monitoring has already been achieved at scale with deployments of AeroScope units across all controlled aerodromes.

Integration of Broadcast Wi-Fi RID has also been achieved in a UTM environment. In November 2018, DJI together with its partner Altitude Angel, demonstrated how Broadcast Remote ID can be integrated into UTM and ATM systems in order to manage traffic at and around busy Manchester airport in the United Kingdom. The trial, called Project Zenith, was a success and showed that all that's needed to bring Broadcast Remote ID into a UTM and ATM environment is to network the receiver, not the drone itself. Notably, one solution for bringing manned aircraft into UTM is likely ADS-B, a broadcast solution that is networked on the receiver end. Broadcast technologies are compatible with, and help enable, a future UTM environment.

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

It should be a requirement that the manufacturer not enable changes to the RID information by customers. In addition, there should be penalties for anyone falsifying or spoofing an incorrect RID.

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

If Broadcast Remote ID is adopted using the ASTM standard, the costs for the vast majority should be zero. All manufacturers selling in the US must already have the firmware to enable RID in place for any product being sold in the US after September, 2022. However, hobbyists

with kit-built drones and older drone models for which manufacturers are no longer providing firmware updates would need a broadcast module to comply.

If Network RID becomes a requirement there will be significant costs for building a system. Those costs will either be borne by the taxpayer or be passed through in terms of costly fees to users. It is worth noting there is already high levels of concern over registration as a means of cost recovery. The FAA speculated that costs for a network remote ID system could be USD 582 million. DJI commissioned an economic analysis by Dr. Christian Dippon of NERA Economic Consulting that put the total costs at more like USD 5.6 billion over a decade.

In addition, if Network RID were required, there are questions of what entity would operate the system. If it is left to the market, it is uncertain if there would be takers willing to supply RID services and even less certain that drone operators would comply. If it is paid for by government, the set up and ongoing costs will either be borne in perpetuity by government or passed on to operators. Again, drone operators may well vote with their feet when faced with high charges and simply not comply. This would be a terrible outcome.

With broadcast RID, most operators will never even have to think about it. When they update their firmware, they will automatically be in compliance. The signal uses the same hardware as the command and control link. Disabling that signal would render the drone unflyable.

There is also the issue of limited network coverage in Australia. This issue is too well understood by anyone who has ventured outside of the major cities to warrant too much discussion, but it is certainly a strong argument against mandating Network RID.

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

If Broadcast is an option, all drones with a certain threshold of capability should be included (except those who fly at aeromodelling clubs for reasons stated previously). If Broadcast is not an option, there should be serious thought to costs associated and what types of users need RID. But limiting the pool of RID compliant users would seriously undermine enforcement and accountability objectives.

Defining the capability threshold of drones included should be done to weed out toy drones, etc that should not be the focus of RID. The FAA's 2017 UAS Aviation Rulemaking Committee on Remote Identification and Tracking ("2017 ARC") had a working group of air traffic, law enforcement, and national security members that considered the question of what UAS should be required to perform Remote ID, and concluded that UAS with either of the following characteristics should comply with remote ID and tracking requirements:

1. Ability of the aircraft to navigate between more than one point without direct and active control of the pilot.

2. Range from control station greater than 400' and real-time remotely viewable sensor.

See 2017 ARC Report page 29.

Drones that cannot fly further than 400' should not be the focus of RID regulations and the owner/operator should be easy to locate for this category of "toy" drones due to their limited range.

Broadcast Remote ID could be rolled out relatively easily by major manufacturers (as has already occurred in the US). Hobbyists and others with older drones will need to attach a module for Broadcast RID.

We would recommend a staged rollout that first requires all drones manufactured after a specific date to have RID capability. Manufactured is the preferred metric, as it would be next to impossible for a manufacturer to ensure drones sold on a specific date are compliant as there

could be old stock still available at retailers. We also think shifting the burden to retailers is impractical as the technical implementation is not within a retailer's control. A second phase, 12 months later, could then require all drone operators be compliant with the RID rule. This would give operators 12 months to understand if their device manufacturer would update their drone or if they needed a third-party device to broadcast the ID signal.

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

ASTM F3411. This standard has formed the basis for rulemaking in the US, Japan and EU (the ASD-STAN standard is essentially very similar to ASTM F3411). If Australia wants to align and to grab low hanging fruit and avoid over complicating RID for manufacturers, users, and its own regulatory and policymaking bodies, it should adopt this standard. The hard work put into this over the past 4 years should not be duplicated. In addition, any manufacturer selling drones in the US past September 2022, would already have a solution in place to meet the US requirement. This means that the rollout for Australia should be simple for the vast majority of manufacturers if the Broadcast variant is adopted.

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

We would encourage the Department to liaise with the US Federal Aviation Administration, the European Union Aviation Safety Agency, and Japan's Civil Aviation Bureau as all three have implemented Remote ID rules. Of the three, the FAA and JCAB would have the most in-depth experience in implementation. We would also encourage conversations with the ASTM and ASD-STAN standards development bodies regarding the respective standards.

Any consultation with telecommunications firms or any other private sector actors, such as prospective UTM service providers, should consider the commercial interests involved.

DJI appreciates the opportunity to comment on the draft proposal. If there are additional questions or further comment we can give to assist, please let us know.

Yours,

Adam Welsh

Head of Global Policy

DJI

Adam.Welsh@DJI.com