# Submission 97 – Response to Remote Identification Discussion Paper

The Remote Identification (ID) Discussion Paper [Remote ID DP] for Public Consultation proposes the use of Remote ID for drones to “improve safety and enable responsible and accountable drone use”.. This discussion paper presents why Remote ID may not actually meet these goals and introduce safety problems and create accountability issues. It also discusses other potential negative impacts of the introduction of Remote ID.

16/07/2023

**Response to Remote Identification Discussion Paper**

**1. Introduction**

The Remote Identification (ID) Discussion Paper [Remote ID DP] for Public Consultation proposes the use of Remote ID for drones to "improve safety and enable responsible and accountable drone use" This discussion paper presents why Remote ID may not actually meet these goals and introduce safety problems and create accountability issues. It also discusses other potential negative impacts of the introduction of Remote ID.

**2. Scope**

For policy discussions it should be noted that Civil Aviation Safety Amendment (Remotely Piloted Aircraft and Model Aircraft—Registration and Accreditation) Regulations 2019 [F2019L01027ES-1] estimates that there are over one million drones in Australia.

This discussion paper comes from the perspective of an Engineer with a background in the field of Telecommunications and the Parent of Recreational Drone Operator.

Remote ID is considered to consist of the following data (based on the FAA standard for Remote ID): Drone ID, Drone location and altitude, Drone Velocity, Control Station location and elevation (i.e. the position of the operator) and a time mark.

This discussion paper is primarily focussed on Broadcast Only Remote ID (BRID). Networked Remote ID is considered as unimplementable for most recreational drones due to physical restrictions (weight/size), cost and the wide range of geographical locations/terrains that have no network connection possibilities. Current standards only support BRID.

**3. Data integrity**

In information Technology there are five pillars of information assurance:

1. Availability: Information is ready for use at the right level
2. Integrity: Guarantees information is accessible or modifiable by authorised users.
3. Authentication: Ensures users are who they say they are.
4. Confidentiality: limits personally identifiable information / classified corporate data.
5. Nonrepudiation: Individuals cannot deny action because system provides proof of action.

A system such as Remote ID needs to meet ALL of the above pillars for the data to reliably considered as valid. However current BRID systems only meet item 1, availability.

A fundamental problem with identification in digital technologies is the issue of ID spoofing. That is where an actor presents themselves as someone else. BRID has already been spoofed. An Internet Search on "Drone Remote ID Spoofing" results in numerous Youtube videos and articles on how this may be achieved.

It is possible using freely available software and cheap general-purpose hardware to broadcast a Remote ID with information indicating a fake identity, fake pilot location and fake Drone location. Specialist skills are not required to do this. Spoofing does not depend on a drone being flown.

This means that 2,3,4 and 5 regarding information assurance cannot be met which leads a fundamental problem with trust in a Remote ID system.

### 3.1 Data integrity safety issues

With a spoofing device it is possible to present one or more (a swarm of) Drones being in the air when in fact there are no drones there. The [Remote ID DP] / clause. 5 indicates that Remote ID could help increase situational awareness. In a spoofing scenario it may decrease this awareness. Due to data assurance issues Autonomous Drones cannot rely on BRID data alone for navigation decisions. If the BRID information of one drone (e.g. GPS location and/or velocity) is spoofed it could lead another a drone to take undesired action, e.g. non-delivery in the case of last mile delivery etc. Incorrect BRID information could also stem from an out of specification component due to a previous hard landing etc. As such an autonomous drone is required to have other sensors e.g. RADAR/LIDAR to maintain situational awareness. If BRID is introduced the Drone operator (autonomous or human piloted) needs to reconcile BRID data and what local sensors are telling them. If the data is inconsistent, what do they do? Which data do they trust?

Using Remote ID as a technology for detecting drones within an air space is also problematic due to data assurance issues such as those introduced by spoofing. An envisaged use of BRID is for airports to detect drones within their airspace. With BRID spoofing it would be possible to disrupt airport's operations by presenting drone movements within the airspace that are not actually there. What procedures would the airports management or conventional aircraft pilots take? How do they reconcile the BRID data with their local sensors? If they can't visually see the drone/s but the BRID data is telling them there is one (or more) there which data do they trust?

There are other technologies that are better suited for drone detection around important assets such as airports or aircraft. The use of Remote ID would be superfluous when using these technologies and may introduce a hazard if an aircraft pilot/s' attention is taken away from an approach or makes evasive action due to a non-existent Drone/s.

As is indicated in [Remote ID DP] / Annex.3 the use of Remote ID for "Detect and Avoid" (DAA) is not feasible due to complexity and latency issues. The ability to spoof data is another reason why Remote ID is not suitable. It will NOT help situational awareness.

### 3.2 Identity Spoofing

The [Remote ID DP] / clause.5 indicates the use of Remote ID for "helping track illegal or noncompliant drone use and report potentially suspicious drone activity to relevant authorities for further action". The use of spoofing would negate this perceived benefit and potentially lead to individuals being incorrectly accused of a crime. In the case of BRID is it possible to record the Remote ID of a drone being used in a compliant way (e.g. a child flying a drone in a park, a last mile delivery drone making a delivery). This BRID could then be spoofed at another location, e.g. at the airport discussed in the previous clause 3.1. This could lead to investigation/prosecution of innocent people/companies. Bad actors involved in illegal activities can easily pretend to be someone else. Current Remote ID systems facilitate this behaviour due to lack of data assurance.

## 4. Cyber Security

[Remote ID DP] clause.6 indicates privacy and cyber security as challenges for the implementation of Remote ID. Recent data breaches in Australia have highlighted the need for data security. A robust analysis of the potential for nefarious use of Remote ID data and associated register data as well as safe guards need to be studied BEFORE any implementation of Remote ID. Once an insecure system

has been rolled out typically there is no way to fix it other than replacement. A 2nd more secure system would be needed adding more substantially more cost and the replacement of all the version one hardware etc. Compatibility between both versions would need to be addressed.

[Remote ID DP] / Annex 3 already lists Data and System Integrity as a challenge. Clause 3 has shown that the Remote ID system has already been comprised.

[Remote ID DP] / Annex 3 indicates challenges around privacy. This is a complex area that would need analysis by multiple Government agencies beyond CASA. The use of BRID allows anyone to track drone movements leading to various negative consequences. For example, consider last mile drone delivery applications. A person could learn the Remote IDs associated with a particular service provider from a public Remote ID list or it would be possible for someone to record a Delivery Service Provider's drone Remote IDs by stationing themselves near a service providers hub and passively recording BRID data. They could then move to another location and use a phone app to search for the company's drones and track them to a location where the drone delivers a parcel. This may lead unwanted uses of the data. For example:

- It would allow rival companies / activists / individuals to monitor and track a company's drone operations. They could determine who the customers are, trading volumes etc. These activities / data may be commercial in confidence.
- It would allow persons such as reporters to station themselves near a person of interest to see what drone delivery companies are delivering to a person. This may give away information regarding the delivery.
- It would allow potential thieves to track delivery drones and see where they are delivering to in order to secure the payload or drone itself.

There are numerous examples where tracking information such as that given inadvertently through fitness trackers has been used for malicious intent.

Security issues are not limited to delivery service providers. The use of BRID would allow the tracking of drones used by Government agencies such as the police / emergency service / military drones / local Government drones. This could alert the general public and potentially criminals to the use of drones in the area acting as an early warning tool.

Another of the problems of the digital realm is the ease of scaling attacks. One common attack on the internet is the Distributed Denial of Service (DDOS) attack whereby many computers are instructed to send traffic to a computer system in order to overwhelm it. As discussed in clause.3, spoofing BRID allows a very similar attack to occur. It is possible to broadcast that there are many drones at a certain location. That may serve to prevent service, e.g. a delivery provider drone may abort delivery with various consequences, some inconvenient some more major. In the case of a remote hospital receiving vital medicines a non-delivery might lead to fatality. Physically preventing or denying the use of air space by a drone is a much harder to achieve.

The potential for security issues regarding the use of drones has already been recognised by the Australian and USA governments in their calls for bans on DJI drones being used by Government departments. Remote ID provides another vector for monitoring or attack by state actors.

Operational security is a very important activity and is diminished by Remote ID.

**5. Personal Security**

One of the pieces of information associated with BRID is the location of the pilot. Allowing the general public to determine the location of a Drone operator may jeopardise the safety of the operator. As discussed in [Remote ID DP] / Annex 3 community acceptance of drone technologies is important. However, some members of the public are hostile to the use of drones, even when the drones are used in a compliant lawful manner. The advertisement of the location of the pilot, would allow people hostile to drones to find and confront the pilot. You now have a Drone operator trying to deal with a hostile person and having to manage drone safety and personal safety. I have firsthand experience of such a situation. The ABC were filming at our residence and at a nearby park. The Drone operator was granted permission by the local council and was acting in accordance with the CASA drone rules. However, a nearby resident confronted the crew and acted in an aggressive manner due to the person believing the Drone was filming them.

**6. Education and Recreational Use**

It is recognised that Drones and related technologies are important for Australia's future. Whilst CASA necessarily focusses on the commercial sector it does recognise recreational drone use in the Drone Rules. It should be recognised that a large percentage of the estimated 1 million plus drones in Australia are for recreational use and that the users are largely un-represented. There is no National Recreational Drone User organisation with a large membership in Australia. The "Model Aeronautical Association of Australia (MAAA)" is the biggest but its' membership would be a tiny fraction of recreational Drone operators. These recreational users neither have the expertise nor budget to fund lobbyists or be on technical or advisory committees meaning their requirements may not be considered or forgotten. Therefore, it is important for policy makers to give due consideration to this large group of people (potentially 1 in 20 Australians, including minors) when implementing policies around Remote ID.

The current Australian Drone regulations strike a balance when it comes to the recreational use of Drones versus regulation. Although the effective banning of First Person View (FPV) Drone usage outdoors by requiring MAAA membership or CASA registration is an impediment to the drone sector. The cost of membership/registration and the need for flight plans along with area approval and document version control procedures prevent many people from engaging in this part of the hobby. A key requirement for FPV Drone usage is to have an observer responsible for the safety of the flight. This would be good practice for any Drone flight as a pilot is fixated on controlling a drone and may not be aware of other hazards. An observer would have more impact on safety and compliance than a Remote ID.

In order to grow an Australian STEM sector and in particular a drone industry it is important to engage young people in operating, maintaining, and building drones. Moving from ready to fly drones to self-built drones, children learn a wide breadth of skills for the future including (but not limited to):

- Software coding
- Radiocommunication (learning about frequencies, encoding such as LORA)
- Video technologies (video transmission, video codecs (e.g. H.265) )
- Electronics
- Battery technologies
- Avionics
- Composites
- Manufacturing (including 3D printing)

- Responsible citizenship through understanding acceptable uses of technology (i.e. CASA drone rules).

People with such skills will be vital for Australia's future. Attendance at the Australian Air Show and Australian Manufacturing Week showed clear innovation in Drone related technologies and in particular their use in Defence. In deed the Australia Army sponsors FPV drone racing in the hope of attracting young pilots and interest in the area.

Any Remote ID policy framework needs to consider that there are self-built drones. Any Remote ID regime MUST not prevent individuals from building compliant drones (either explicitly nor implicitly, e.g. through expensive compliance testing).

The cost, regulatory barriers and privacy/security/safety issues surrounding Remote ID make Drone operation unattractive. The cost of the Remote ID scheme may be better spent on expanding the "Know your drone" program to one that provides material to schools (or visits them) about the benefits to society of drones as part of a drive for greater STEM adoption at schools. Being able to show:

- How Drones benefit various sectors such as agriculture, health and defence
- Various technologies used in drones
- Responsible use and how they interact with society

will encourage discussion in families and the community leading to a greater acceptance of Drones and more interest in STEM. This may provide a cheaper and more positive way of achieving public education and compliance goals rather the stick approach of penalties related to non-compliance to Remote ID.

Adding additional hurdles to the uptake in young Drone enthusiasts and recreational users is detrimental to Australia's future. Having a vibrant STEM/Drone industry is more valuable to Australia than being able to prosecute a few non-compliant Drone operators.

**7. Areas designated for Drone use**

Limiting non-Remote ID Drone use to certain geographical areas is problematic for recreational users. For child Drone Operators this would rule out the local park as a place to fly their drone. They would require transport including time to and from an authorised area adding to the cost of operation. This would be an impediment to the uptake of Drones and encourage non-compliance. Other scenarios such as using a drone to cast a fishing line on a remote beach would make operators non-compliant. There are myriad of scenarios where drones are used that present zero danger to the public.

Having a centralised area where many drone operators are forced to fly would increase the incidence of radio interference and increase the chances of collisions / crashes / fly aways etc. This has the potential to cause conflicts between operators as well as locals resenting the noise from many drones. This would increase the negative view of drones.

Having a large concentration of drones in one place, would also offer a "honey pot" for hackers to steal Drone Remote ID data to be used for later nefarious activities.

There would need to be procedures for the definition of areas designated for Drone Use as well as ongoing oversight and review procedures. Who would define these areas? On what basis? What criteria would need to be met? What would be the relation between the various stake holders: drone operators, land owners, nearby residents, Local, State and Federal Government departments? The work required to define these zones would add to the cost of implementation of Remote ID.

**8. Cost**

[Remote ID DP] clause.6 identifies 3 costs of Remote ID, namely:

i. Existing drone operators would need to add Remote ID equipment to their drones.
ii. Different parts of the drone sector may be disproportionately impacted (e.g. particular drone users or types of operations).
iii. Responsible Government departments and agencies may need additional resources to develop, implement and enforce Remote ID requirements.

This appears to downplay the cost of such a scheme.

Item **i.** indicates that existing drone operators would need to add Remote ID equipment to their drones. This is not an insignificant cost given that there are over 1 million drones in Australia. Adding Remote ID may be possible for commercial drone operators being a small subset of user however it would not be possible for all recreational users to retrofit their drones. There are various reasons for this such as: limited technical no-how, no physical space, hardware incompatibilities and unawareness of the need for Remote ID. There is the personal cost of having to buy a new drone, environmental cost of throwing away the old one away and potential cost of being non-compliant. The overall cost of hardware compliance for Remote ID by recreational Drone operators would be in the hundreds of millions of dollars to retrofit or replace existing drones. The addition of Remote ID hardware on every drone will drive up the cost of each drone in new Drone purchases. NRID would impose more cost due to additional network connection technologies and network connection costs. There is also the potential for a Remote ID registration fee. [F2019L01027ES-1] has highlighted CASA seeking a levy for Remote Piloted Aircraft registration in the past. As implementation costs of Remote ID would be significant there is a temptation to recover costs from future Drone operators.

The use of "may" in item **iii.** appears to be incorrect, additional resources WILL be needed. [Remote ID DP] / Annex 3 alludes to this in several clauses:

Mitigating Airspace risk: There would need to be significant investment by both the government and private sector to research, develop policy frameworks, compliance frameworks and implement (hardware, software, human capital) to implement any scheme to mitigate airspace risk.

Informing Policy and Regulation: There is a cost to develop the policy framework and regulation. [Remote ID DP] / Annex 3 highlights initiatives and activities associated with this.

Community education: In order to implement Remote ID a significant advertising campaign would be needed with associated cost. There may be ways of mitigating the cost by limiting RemoteID to a subset of drone users. As highlighted in clause 6 this money may be better spent on a broader benefits of STEM/Drone campaign and educating users on usage and potential issues. A positive campaign rather than a negative "follow the rules or you'll be punished" campaign which Remote ID seems to be facilitating.

Conformance monitoring/enforcement: It is important to detail impacts to all government Departments (not just CASA) to determine the cost. The use and impacts of Drone Use and Remote ID would need to be communicated at all levels of Government and through multiple Government Agencies.

[Remote ID DP] does not discuss the cost of securely maintaining Remote ID data and information assurance (or lack of) associated with it. The monetary cost in securing the data is not insignificant.

The preceding clauses also allude to intangible costs. For example: what is the cost to the aviation, business and the community in the cases of spoofing?

Cost is a major issue. Remote ID is uneconomic given minimal real benefit.

**9. Clear Requirements**

In developing policies and protocols, it is essential to clearly define requirements.

The Department of Infrastructure is to be applauded for implementing a public consultation process on Remote ID. The Remote ID discussion paper is one part of the process to potentially introduce Remote ID. It is important that statements from the discussion paper do not simply find their way into subsequent documents without analysis/scrutiny.

One of the main drivers of Remote ID appears to be identification of operators using drones in an unsafe manner. The Remote ID discussion paper provides no data on the scope or breath of this issue.

Drone Fast Facts (hΣps://consultation.casa.gov.au/regulatory-program/dp1708os/supporting_documents/Drone%20factsheet_final%20proof_web.pdf) from CASA indicated that in 2017 CASA has issued 20 aviation infringement notices and educated 400 people about their need to comply with the rules. Based on 1 million drones and using these figures 0.002% of drones are infringing per year. Hardly an epidemic of bad behaviour.

Is it increasing each year? What new incidents require the use of Remote ID? [[F2019L01027ES-1] (2019) describes incidents in other countries but indicates no deaths or serious injuries in Australia.

To facilitate informed discussion on the need for Remote ID it would be good for all stake holders to have a current picture with respect to non-compliant Drone usage in Australia. Yearly data could instruct any trends. This would allow data on the effectiveness of the "Know Your Drone" and other educational programs.

Furthermore, it would be beneficial to be presented with some analysis of instances of infringement/non-compliance. This analysis should also indicate whether the Drone operators would have modified their behaviour if there was a Remote ID. For example: [F2019L01027ES-1] reports a collision with a race participant and a Drone filming the race [CASA AR-2017-016] (hΣps://www.atsb.gov.au/sites/default/files/media/5773362/ar-2017-016a_final.pdf). Would the incident not have occurred with Remote ID?

Through this data a proper cost / benefit analysis could be provided. It may be uneconomic to introduce Remote ID for a marginal increase in compliance given the overall cost of implementation.

An even more basic driver it seems is that CASA does not accurately know the number of Drones in Australia and is using Remote ID to determine the number of drones more accurately. The cost of 100s of millions of dollars to the Drone sector to determine this number does not seem economically rational way of determining this figure.

Each of the uses and benefits outlined in [Remote ID DP] should incur a similar level of analysis to see that Remote ID is fit for use.

**10. Standards**

[Remote ID DP] clause 8 requests input on the use of existing standards and in Annex 2 it specifies two standards: FAA ASTM – F3411-19 and EASA ASD-STAN prEN 4709-002 P1. It is not possible to

comment on prEN 4709-002 P1 as the cost of 250 Euros to download the document is prohibitive for a recreational user. The comments in this discussion paper thus have focussed the FAA implementation of Remote ID. The preceding clauses have shown significant issues in this standard and why it is not suitable for implementation in Australia.

Implementing a Remote ID policy and standards at significant cost in order to evaluate how it could be used in the future for an evidence base is bad policy and bad engineering. This discussion paper highlights existing problems with information assurance, security and the high cost of rolling out the scheme. To fix problems would require a new physical rollout to all Remote ID mandated drones. It would be irresponsible to mandate the use of a standard with known issues.

The question then is should Australia define their own standard?

Whilst a more robust solution may be found, the economics surrounding this are questionable. Industry would need to be involved in any such specification leading to the creation of a working group to define requirements, frameworks, protocol/s, test suites and conformity documents. This working group would have to meet multiple times and have input from all the relevant stake holders: drone manufacturers, various industries utilising drones, cyber security experts, privacy experts and a diverse set Government Departments (Australian Communications and Media Authority, Australian Signals Directorate, Civil Aviation Safety Authority, Department of Industry, Science and Resources, Department of Infrastructure etc.). These stake holders would have to have the budget and time to devote to the activity.

Buy in from manufacturers (typically based in China) would be questionable. Australia is a limited market and it may not make economic sense to be involved. If a standard was developed the cost per unit for any hardware associated with the Australian Standard implementation would be high in order to capitalise on any investment in the limited market.

Due to the nature of Australian Standards not being freely publicly available (unlike many standards from International Standards Development Organisations) the process is unlikely to get buy in from recreational Drone operators and education due to the cost involved.

It is recommended NOT to pursue a domestic Australian standard for Remote ID without fully understanding the requirements and doing a cost/benefit analysis. Other targeted methods to determine the number of drones in Australia, increase compliant drone usage and increase situational awareness may be better and more cost effective.

**11. Usage**

[Remote ID DP] clause 8 item 11 requests feedback on "Should mandatory equipage be rolled out to all drone operators, or phased through types of operators and/or operations?".

The above clauses have highlighted issues with the implementation and usage of a Remote ID system showing that mandating the use of Remote ID in all Drones in Australia does not meet the goals of the stated uses and benefits. Its' implementation would be at a high cost and harm the Drone sector. It is simply not feasible to retrofit every one of the 1 million+ drones to be compliant with Remote ID making thousands of ordinary citizens who have been following the existing Drone rules open to prosecution.

Some of the challenges could be mitigated making the use of Remote ID mandatory in some classes of drones and not in others. For example: Drones operated by Government Departments (such as the Military or Police) or Delivery Service Drones may turn of Remote ID to prevent tracking. However

that negates the perceived benefit of situational awareness as some drones (probably large ones) have no Remote ID whilst other classes do have Remote ID. Therefore, it would be useless to rely on Remote ID data to make navigation or compliance decisions and some other more reliable method would be needed. Remote ID would be superfluous and increase cost for no benefit.

A system that requires a mandatory Remote ID on subset of drones as opposed to all Drones would incur very similar costs at a Governmental level and business level. The costs required to formulate policy and implement Remote ID would be similar for 5000 vs 100,000 drones. The same level of security and privacy and oversight is needed at the outset of the scheme. There is a smaller variable cost as the data grows. Business would be required to consider and act on the scheme adding to their costs. There would be a piecemeal unreliable system at high cost.

From a recreational Drone operator perspective this discussion paper does not support the use of Remote ID for this class of uses.

**11. Conclusion**

Drone usage in Australia is a complex issue with many types of operators with complex and varied types of operations. This discussion paper highlights many issues and concludes that the mandated use of Remote ID is a costly and problematic exercise with questionable benefit and is NOT fit for purpose in Australia.

Therefore, the 'NO ACTION' policy option is supported and it recommended to pursue other policies/technologies in order to meet use/benefit objectives.