OFFICIAL



Transport group / international aviation, technologies and services division / safety and future technologies branch

Emerging Aviation Technologies Policy Forum

Workshop on Remote ID meeting summary

August 2024



© Commonwealth of Australia 2024

August 2024 / INFRASTRUCTURE 2024

Ownership of intellectual property rights in this publication

Unless otherwise noted, copyright (and any other intellectual property rights, if any) in this publication is owned by the Commonwealth of Australia (referred to below as the Commonwealth).

Disclaimer

The material contained in this publication is made available on the understanding that the Commonwealth is not providing professional advice, and that users exercise their own skill and care with respect to its use, and seek independent advice if necessary.

The Commonwealth makes no representations or warranties as to the contents or accuracy of the information contained in this publication. To the extent permitted by law, the Commonwealth disclaims liability to any person or organisation in respect of anything done, or omitted to be done, in reliance upon information contained in this publication.

Use of the Coat of Arms

The Department of the Prime Minister and Cabinet sets the terms under which the Coat of Arms is used. Please refer to the Commonwealth Coat of Arms - Information and Guidelines publication available at [http://www.pmc.gov.au](http://www.pmc.gov.au/).

Creative Commons licence

With the exception of (a) the Coat of Arms; and (b) the Department of Infrastructure, Transport, Regional Development, Communications and the Arts photos and graphics, copyright in this publication is licensed under a Creative Commons Attribution 4.0 Australia Licence.

Creative Commons Attribution 4.0 Australia Licence is a standard form licence agreement that allows you to copy, communicate and adapt this publication provided that you attribute the work to the Commonwealth and abide by the other licence terms.

Further information on the licence terms is available from <https://creativecommons.org/licenses/by/4.0/>

This publication should be attributed in the following way: © Commonwealth of Australia 2024

Contact us

This publication is available in PDF and Word format. All other rights are reserved, including in relation to any departmental logos or trademarks which may exist. For enquiries regarding the licence and any use of this publication, please contact:

Director – Internal Comms and Creative Services

Communication Branch

Department of Infrastructure, Transport, Regional Development, Communications and the Arts

GPO Box 594

Canberra ACT 2601

Australia

Email: publishing@infrastructure.gov.au

Website: [www.infrastructure.gov.au](http://www.infrastructure.gov.au)

# Background

## The Emerging Aviation Technologies Policy Forum

The Emerging Aviation Technologies Policy Forum provides a mechanism to help inform the development of policy advice for emerging aviation technologies in Australia.

It is the principle forum for the lead aviation policy agency, the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (the department) to consult with a range of stakeholders.

The forum is not a decision-making body. It is intended to be a mechanism for open, non-binding discussions on policy options and associated issues. It does not replace broader industry consultation by other agencies’ working groups or forums.

## Purpose of the workshop

An Emerging Aviation Technologies Policy Forum workshop was held on 5 July 2024 to hear from members’ experience and insights to help inform options for Australia to implement a Remote Identification (Remote ID) mandate for drones.

The workshop covered options for no Remote ID mandate, and mandates for broadcast, network or hybrid approaches to Remote ID. Participants were asked about the practical realities of bringing in a Remote ID mandate and what impact it would have on their business or drone use.

The comments summarised in this paper reflect feedback from workshop participants and do not represent the view of the department or the government.

# What we heard

## General comments

### Be clear on the problem being solved

One area of focus, where many participants had similar feedback, was that there needs to be a clear explanation of the policy problem Remote ID is intended to solve.

Key comments from participants included:

* Remote ID is primarily for identification.
* Safety is not sufficient to be the policy motive as Remote ID technology is not advanced enough to offer airspace deconfliction or integration.
* A secondary benefit is for post-flight data gathering, which can then be used to help improve situational awareness, conformance monitoring and air risk analysis.
* Remote ID doesn’t enable international harmonisation because;
	+ Australia won’t automatically adopt the details of Remote ID used in other countries, noting that over 40 countries have a Remote ID obligation and many use slightly differing standards.
	+ A Remote ID mandate would impact tens of thousands of domestic businesses, while benefitting tourists and potentially multinational companies.
* Three reasons for considering a Remote ID mandate were anonymity, congestion and the rapidly changing nature of drone capability. These reasons aren’t effectively addressed by the options of Network ID, Broadcast ID or a Hybrid of the two, however, they can support a full Uncrewed Traffic Management (UTM) solution which may address these reasons.
* Several participants noted that ‘license plates for cars’ is not a good analogy for how Remote ID technology works and its subsequent impacts, and that use of this analogy may be misleading for policy decisions on implementing Remote ID.

### Clarity of purpose will drive when and what action will be needed

Participants were keen to better understand the primary policy issues, and wanted to see the data that supports action needing to be taken and whether Remote ID is the appropriate tool.

For example, what are the numbers of non-compliant users or drone uptake? Are there other industry-led mechanisms achieving a similar result? Could targeting other airspace users (e.g. ADS-B on all crewed aircraft) fix the problem?

### Remote ID is a complex choice

Participants suggested a range of other issues that need to be considered in developing Remote ID policy options.

* What identification data is being transmitted?
* Who would use this data?
* What privacy safeguards would be in place?
* How would compliance be enforced? Look at compliance rates overseas and whether introduction was delayed for any reason.

There are many options for implementation, some participants recommended the department develop use cases and explorations of specific scenarios.

### Details on data requirements will affect cost and implementation timeframes

* Cost to operators must be weighed.
	+ Remote ID devices compliant to Federal Aviation Administration and European Union standards are already below $150 per drone, but that can still be a substantial cost. Swarm light show operators in particular have hundreds or even thousands of drones.
* Industry is likely to need more than two years to implement a response to the mandate of any Remote ID option.

## Discussion around the four options

Participants raised multiple differing views on all the options discussed. These views are captured below, at times the views may appear contradictory as different individuals had different perspectives.

### No mandate

**In support of no mandate:**

* Australia has driven many innovations in UAV technology worldwide, and bringing in Remote ID may limit future innovation by driving up cost and potential for competitors to gain insights into testing.
* Assuming Remote ID is primarily for electronic conspicuity, there are other industry-led technologies or systems that can achieve it, such as ADS-B.
* Security is important, bad actors can falsify a Remote ID.
* Awareness and compliance with the know-your-drone rules is important, government agencies and companies could do their own awareness campaigns to improve compliance.

**Against no mandate:**

* Although bad actors can interfere with Remote ID, it can still shape behaviour;
	+ It’s highly likely some non-compliance with rules and regulations is out of either ignorance or a willingness to ‘cut corners’, knowing that your drone can be identified can be a powerful motivator to people to learn how to follow the rules.
* Drones in densely populated areas of Australia can cause fear for some in the community.
* Those flying crewed aircraft are concerned it is ‘only a matter of time’ until an incident happens.
* Industry is very unlikely to opt-in to using a Remote ID if given a choice.

### Broadcast Remote ID

**In support of Broadcast Remote ID:**

* Broadcast ID is often cheaper for the operator because they don’t need to pay for network connection or have a sim card.
* New drones are often fitted with Broadcast ID (noting there is a cost to the manufacturer when it gets fitted) so there is little effort required for compliance.
* It is lower cost than network Remote ID (e.g. no infrastructure needed) and it can continue to operate outside existing network coverage.
* If the intent is to be able to pull phone out and get understand if there are other drones in the area, Broadcast Remote ID should be sufficient.

**Against Broadcast ID:**

* Blue-tooth is short range and of least use in built up environments like cities.
* May require significant investment in on-ground infrastructure with significant costs.
* Bad actors could block system.
* Broadcast is unlikely to enable granular airspace data collection.

**Other things to consider:**

* Broadcast Remote ID range is approximately 1km, human eyes can see further.
* Broadcast ID may be more appropriate in rural areas or for high volume camera drones.

### Network Remote ID

**In support of Network Remote ID:**

* Network Remote ID could be used to match areas where the congestion is greater (this often coincides where there is network connectivity – i.e. urban areas).
* The technology may improve community confidence in drones, for some members of the community who have little experience with drones.
* Network ID data can help build a robust data set about drone flights in Australia to help optimise future business operations and regulations.

**Against Network Remote ID:**

* United States of America didn’t include Network ID for cyber security reasons.
* Ongoing cost, unclear about the requirement for private software providers.
* The implementation burden falls heavily on industry.
* There is a risk to drone pilots, as fellow drone flyers may be able to gather data on them or their operations from the supporting software systems.
* Network ID may stifle innovation, as users may be less willing to conduct trials or operate in new areas if they felt their data could be accessed by competitors.

**Other things to consider:**

* A lot of areas in Australia do not have 4G/5G coverage, it is not possible to have an Australia-wide Network ID solution.
* Potential for Australia to explore the use a height corridor/sky highway model, similar to parts of both Japan and the UK.
* In principle, the burden of the implementation cost should be borne by users.

### Hybrid model

This approach sparked significant discussion and raised issues such as:

* A hybrid model should be risk based and where there is demonstrably a clear benefit. This could look like:
	+ Place-based mandate;
	+ Mandate based on drone specifications (e.g. beyond line of sight operations, heavier drones or drones with a hazardous mandate).
* A Remote ID mandate should be purpose and use case driven, working through practical applications.

# Next Steps

* Further detail on potential options, incorporating participant feedback to be considered by Remote ID workshop participants by Q4 2024.