Submission 145 – Australian Association for Uncrewed Systems (AAUS)

28 July 2023

AAUS Submission to Public Consultation on Remote Identification Discussion Paper

The Australian Association for Uncrewed Systems (AAUS) is pleased to provide this submission to the Department of Infrastructure, Transport, Regional Development, Communications, and the Arts' (the Department) discussion paper on Remote Identification (Remote ID).

About AAUS

The Australian Association for Uncrewed Systems is Australia's oldest and largest industry advocacy group for drones and the emerging Advanced Air Mobility (AAM) sector. AAUS is a not-for-profit organisation which represents the drone and AAM industry across three domains: land, sea, and air. AAUS' objective is to promote a professional, safe and commercially viable uncrewed systems and AAM industry. AAUS achieves this through its industry advocacy and promotion, education and outreach, and networking activities.

AAUS provides a single representative voice for the full breadth of the drone and urban AAM industry. AAUS' 3,000 members span small-to-large enterprise, manufacturers, licensed and unlicensed operators, training providers, academic institutions, Government, and other supporting technical and professional services in the Australian drone and AAM industry.

General Feedback:

Since commenting on an earlier draft of this Remote ID discussion paper, AAUS has invested significant time and effort on activities to build a more considered position. Activities have included a membership survey, discussion amongst AAUS membership advisory groups and other industry stakeholders. Results from our membership survey are included in the appendix.

Generally, support and feedback on the potential use of Remote ID was mixed and AAUS believes that this stems from an absence of a clear vision on what outcome we are trying to achieve with this technology and how it fits into the broader UTM and technology architecture.

For instance:

- Is the desired outcome one of airspace protection? If so, how this intended to work alongside the National Drone Detection System?
- Is the desired outcome one of airspace situational awareness? How does this work in Class G airspace where general aviation does not have a mandate to equip?
- Is the desired outcome to address security concerns?
- Is Remote ID a necessary building block for UTM? If so, does the technology solution require network based Remote ID (NRID)?
- Is registration a necessary building block for Remote ID?
- Does the drone industry have a social license problem and, if so, will Remote ID address this issue?
- Does the drone industry have a non-compliant operational problem and, if so, will Remote ID address this issue?

The suitability and factors that need to be considered in relation to Remote ID vary depending on desired use and the higher level "problem" it is intended to solve. In some cases, Remote ID may not be a suitable solution at all and consequently, it is hard to provide meaningful feedback without a clear understanding of the context and intended use.

We understand that much of this work may already be occurring in the background within the Department, CASA and Airservices Australia but very little of it is visible to the aviation industry.

AAUS believes that in consultation with the broad aviation industry, the Australian Government and agencies needs to develop a clear vision around a future airspace framework, airspace integration for drones (including the use of UTM) and drone use accountability to determine the most appropriate technical solutions to implement.

Feedback on key policy considerations:

- Remote ID to benefit airspace situational awareness and safety.

AAUS believes that airspace situational awareness equipage and services for drones needs to be undertaken as part of a broader aviation lens incorporating all aviation stakeholders. Remote ID is a technology applicable to drones only and it is unclear how visible it will be to traditional aviation for the purposes of situational awareness. Standalone Remote ID, as defined today, is not a form of electronic conspicuity.

From that perspective, it makes sense to us that if we want to integrate drones into airspace alongside traditional aviation then we should carry compatible equipage that supports a common awareness of air traffic across all airspace users. It is important to note that current Remote ID specifications have not been verified for use in traffic awareness and separation applications.

The collection and sharing of traffic information could also occur through the incorporation of Remote ID with UTM. It is possible that the UTM System could use Remote ID in a number of possible services for drones and conventionally piloted aviation. There may be benefits for Remote ID in a UTM system to enable airspace information sharing and potentially tactical deconfliction of RPA with other RPA in congested areas. There are numerous factors that would need to be considered if it Remote ID were to be used for this purpose, including but not limited to:

- GNSS accuracy, availability and susceptibility
- Communications performance such as coverage, range, latency, robustness to disruption, and security (e.g., data, spoofing)
- Equipment reliability and assurance

These factors would need to be assessed as an integrated part of the overall UTM system (e.g., UTM service volumes / coverage, latency, accuracy, etc.) against the requirements specific to the UTM service provided (e.g., airspace awareness vs tactical separation, etc.). For this reason, it is not possible to assess the adequacy of Remote ID in isolation of the UTM system.

However, due to its short range, AAUS understands that Broadcast Remote ID (BRID) is not suitable for UTM and for airspace deconfliction purposes. Based on discussions with Airservices Australia, we understand that NRID is a key building block for UTM.

If Remote ID is a necessary building block for UTM, then NRID or other suitable equipage (such as ADS-B) should be mandated for drones and other traditional aviation wishing to operate in a UTM environment and benefit from services such as airspace deconfliction and automated approvals.

This raises questions about the broader utility of UTM where there is no internet coverage or outside of controlled airspace where traditional aviation does not have a mandate to be electronically conspicuous. At least in early implementation, it would seem to limit UTM to areas with internet coverage and inside of controlled airspace, or at very low levels (<400ft).

For greater situational awareness and airspace safety outside of controlled airspace (OCTA), AAUS advocates for an EC mandate for all general aviation and drones operating beyond visual line of sight and has produced a separate position paper[1] on this matter.

Apart from the obvious safety benefit of greater situational awareness in Class G airspace, this has the potential of expanding areas where a UTM could be established into regional areas where Beyond Visual Line of Sight (BVLOS) drone applications could flourish.

For drones operating outside of a UTM environment and within visual line of sight, AAUS does not see significant benefit in mandating a Remote ID capability from the perspective of airspace management and safety.

- Remote ID to benefit accountability, enforcement and security.

  There was concern over the assumption that Government needs to keep the Australian drone industry accountable. Presumably this is related to addressing public concerns and maintaining our social license to operate drones in the vicinity of population centres.

AAUS questions whether there is sufficient evidence of accountability and / or security issues related to drone use in Australia to drive mandatory Remote ID and rejects the use of Remote ID for that purpose.

If the objective of Remote ID is accountability, enforcement and security, there is very little reason to limit it by location or drone user category. This points to a broad mandate for Remote ID and we understand this will come at significant cost to industry and may have several unintentional consequences.

The effectiveness of Remote ID as a "mitigator for security risk" has yet to be substantiated. It is posited that, intentional bad actors would not utilise Remote ID in the first place, reducing the benefit of the system to that of enabling enforcement agencies to distinguish an unknown / non-broadcasting drone from one that is compliant. Benefits in terms of actor identification and subsequent enforcement action would be limited. The system would enable authorities to undertake compliance enforcement and safety promotion / education activities but only for compliant (and likely well intended) operators and not the primary actors of interest.

[1] AAUS Position Paper – Improving Airspace Safety in Class G Airspace through Electronic Conspicuity https://www.aaus.org.au/public/161/files/AAUS%20Board/Advocacy/AAUS%20Position%20Paper%20-%20Improving%20Airspace%20Safety%20in%20Class%20G%20Airspace%20through%20Electronic%20Conspicuity.pdf

We understand that BRID has been mandated by the FAA and EASA and that may offer Australia valuable insights from lessons learnt in those jurisdictions.

AAUS understands that the implementation of Remote ID in the United States has been adversely impacted by the requirement for it to be "tamper resistant". By nature, this requires that drone systems need to be locked down to some degree in terms of configuration (hardware and software). This is problematic for a number of systems and would inhibit operational capacity and may inhibit growth of an indigenous drone capability.

It would also be impractical to mandate Remote ID for recreational users including model aircraft hobbyists. Whilst many recreational users have adopted commercial drones that are already equipped with BRID capability, AAUS understands that many home-built recreational systems do not even carry GPS and would require significant work to comply with a Remote ID mandate.

AAUS understands that there are significant unintended consequences of a broad mandate for Remote ID including inhibiting indigenous capability.

Further, if remote ID needs to exist alongside registration to be able to identify drones and operators, Government will need to re-visit registration for recreational drones.

The effectiveness of Remote ID in this particular use case is tied to the effectiveness of the drone registration scheme (in terms of scope of mandate and participation / compliance).

Conclusions:

- AAUS believes that in consultation with the broad aviation industry, the Australian Government and agencies needs to develop clear vision around a future airspace framework, airspace integration for drones (including the use of UTM) and drone use accountability to determine the most appropriate technical solutions to implement.
- This is a discussion that goes beyond the drone community and goes to the strategic direction of airspace and airspace traffic management for all airspace users. It is AAUS' understanding that the Australian Future Airspace Framework is tasked to develop the strategic vision and roadmap for the Australian Airspace System – inclusive of considerations as it relates to drones, AAM, and alongside the needs of the existing aviation sectors, airports, and the ANSP.
- Before that stage, we recommend **no action** with respect to a Remote ID mandate.
- Remote ID may have a place in a future UTM ecosystem.
- We do not believe that there is sufficient evidence to justify implementation of a Remote ID mandate in Australia based on accountability or security concerns.
- There are potential unintended consequences of a broad Remote ID mandate.

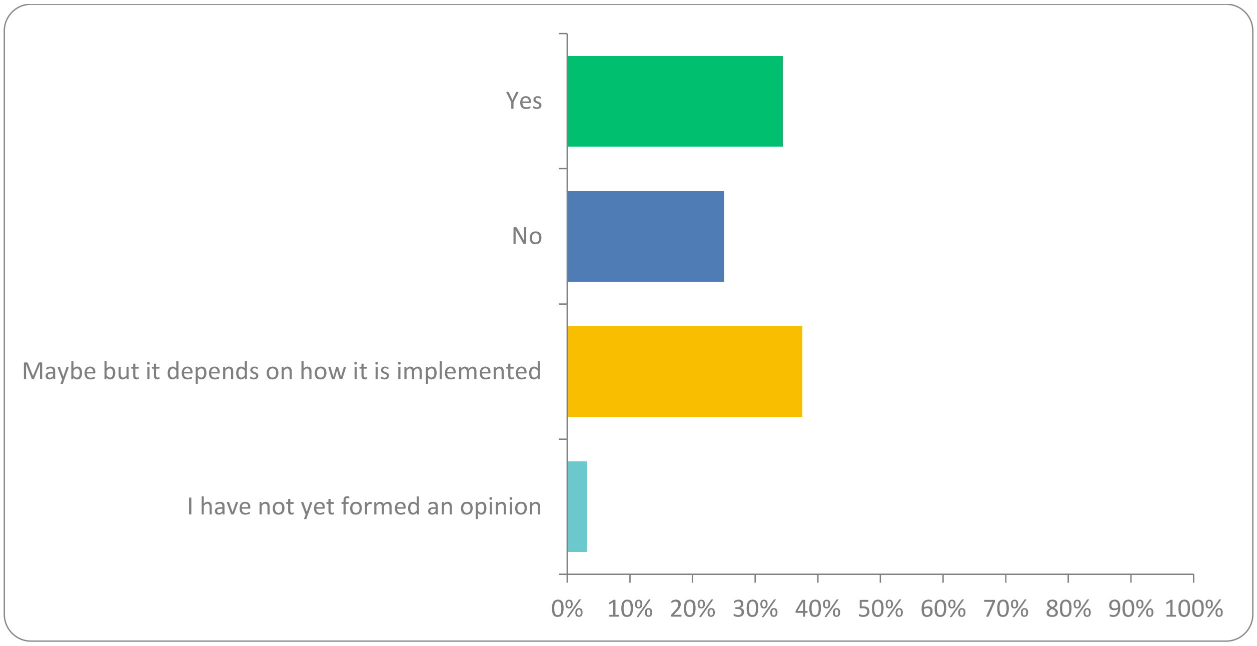
Contact

AAUS would be pleased to provide additional information to the Department on the matters contained in this submission. [redacted]

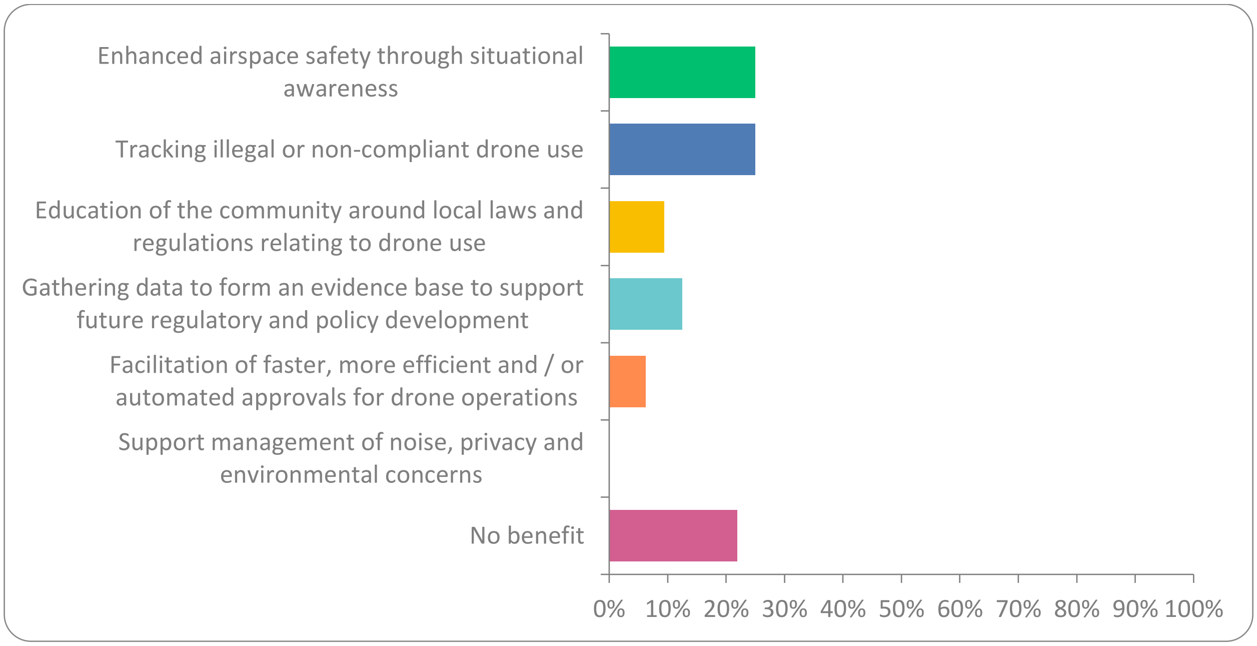
Appendix: Responses from AAUS Survey on Remote ID

Total responses: 32

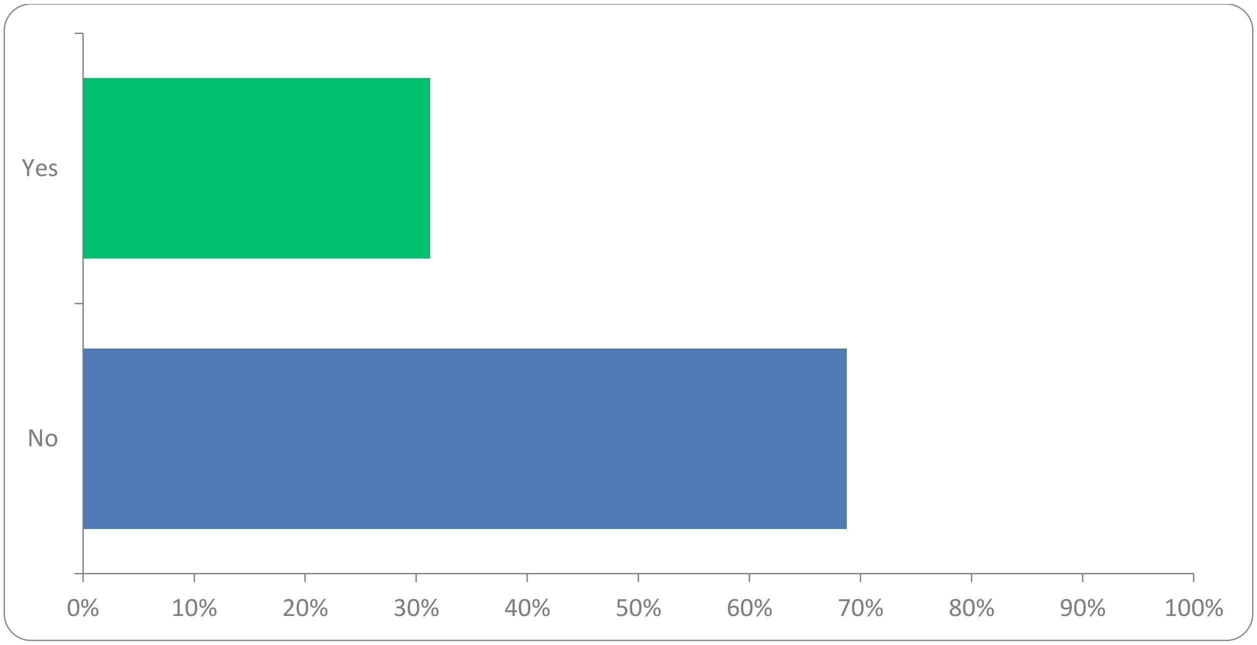
Do you support a remote ID mandate?



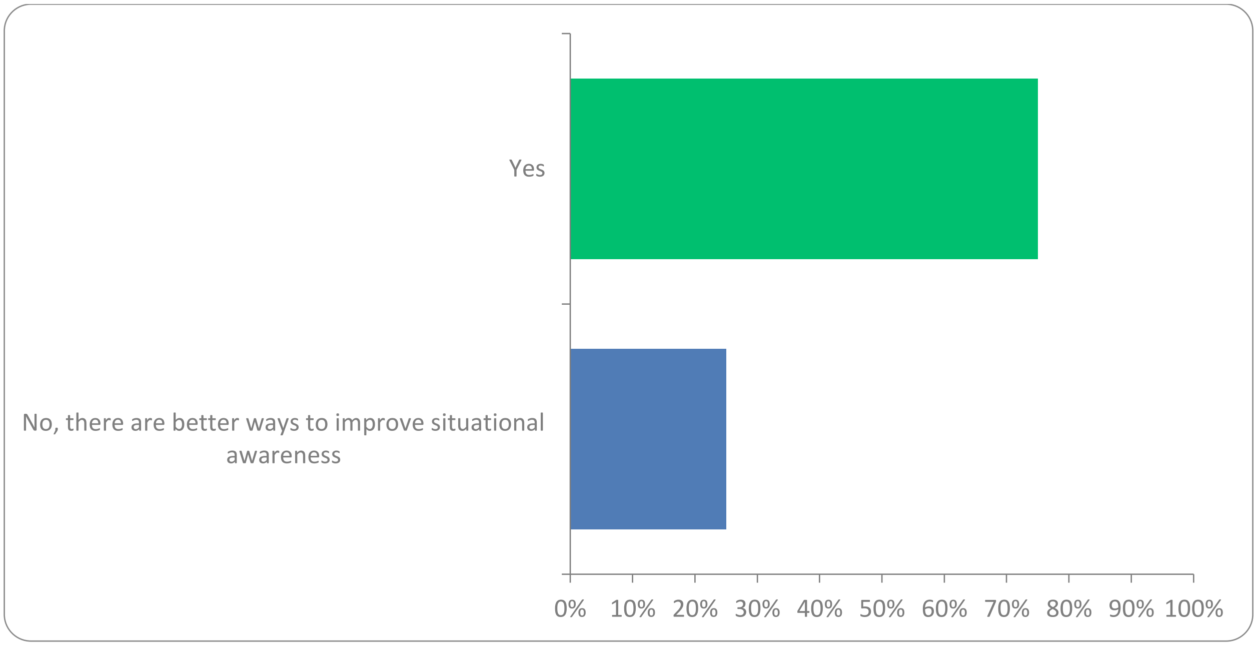
What do you believe will be the major benefit of a drone remote ID mandate?



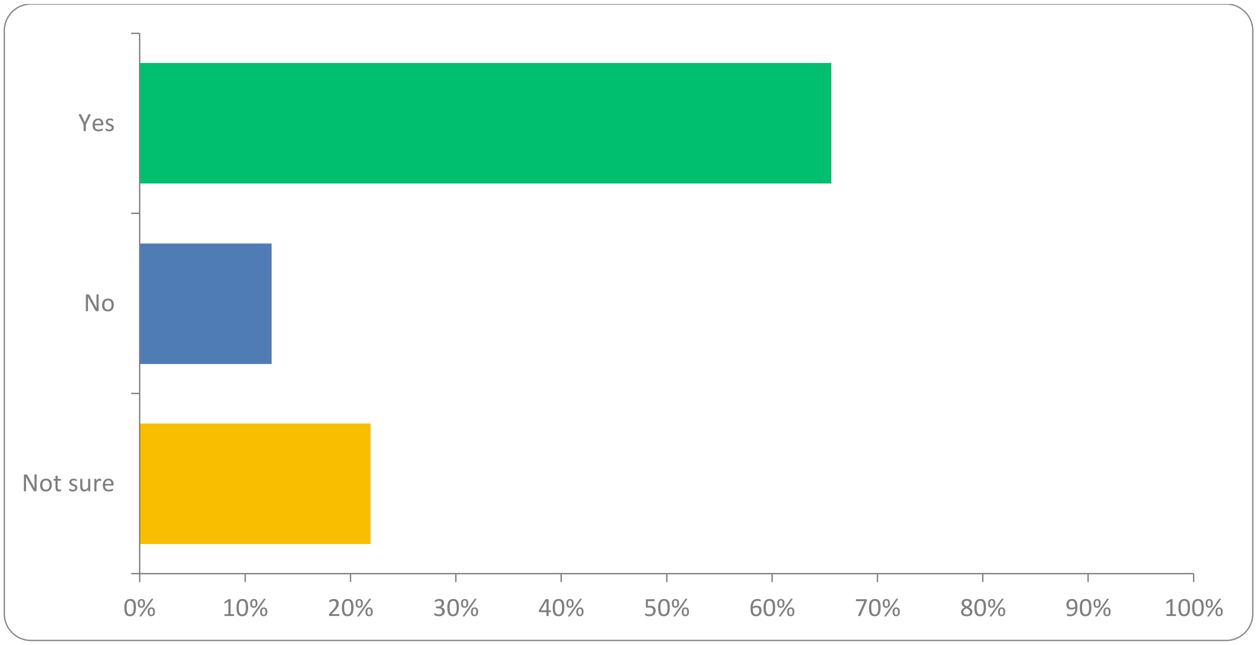
Do you believe that remote ID is necessary for drone operations within standard operating conditions (visual line of site, below 400 ft and clear of people and aerodromes)?



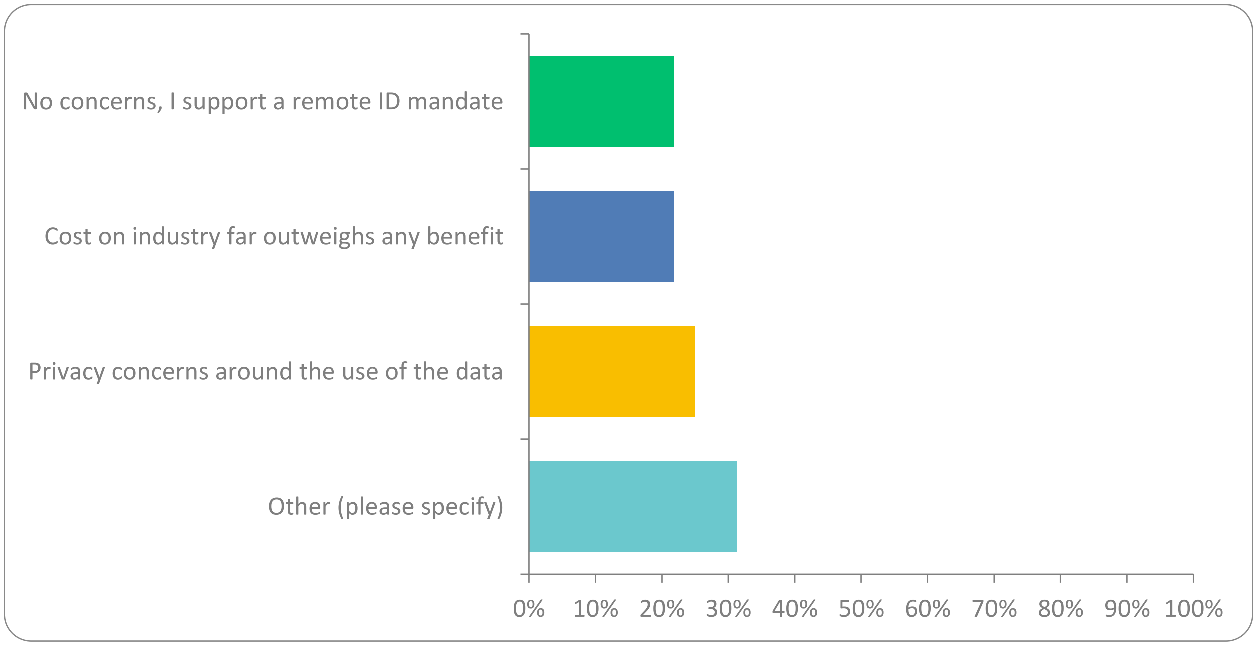
Do you believe that remote ID is necessary for drone operations that are beyond visual line of sight (BVLOS)?



Do you think that a mandate for ADS-B or lower power electronic conspicuity devices for all VFR aircraft and BVLOS drones would lead to better situational awareness in Class G airspace over remote ID on drones?



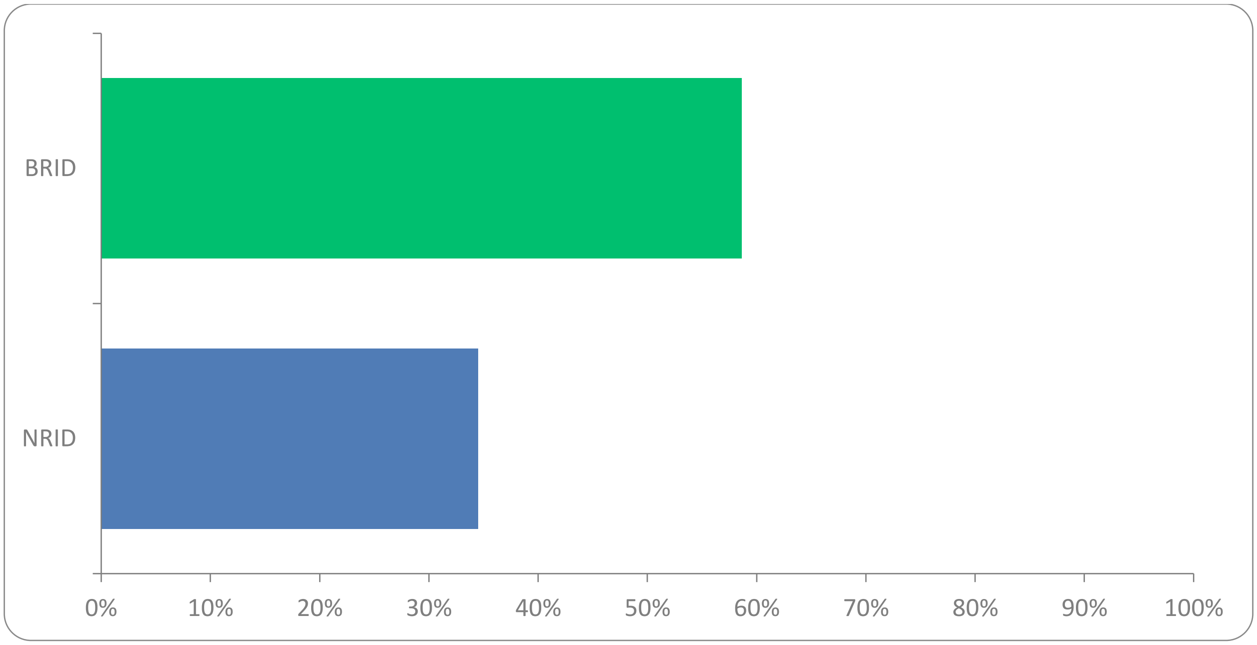
What is your main concern relating to a remote ID mandate?



Other concerns specified:

- *impact on small UAV vendors and ability to maintain vehicles.*
- *The technology design is focused on privacy and security which may shortfall other benefits of Identification Technology (Such as Separation Assurance)*
- *Further unnecessary financial, regulatory, and privacy burden on the hobbyist, or low-risk commercial operator, with most RPAS operators seeing no benefit.*
- *Implementation role out process and community perception. Experience from the US suggests the rollout will NOT be taken well by the majority of recreational users.*
- *why don't we use ADS-B?*
- *Yet again, those who do the right thing will be burdened with more admin & more cost - while those who don't do the right thing will carry on with impunity.*
- *Cost & initial introduction subsidies to drive uptake, coupled with amnesty period for any older non-compatible hardware. Technology, to avoid data & privacy concerns outlined, move to a ADS-B type approach where the ICAO 24 bit hex is registered to the operator, everything else as per ADS-B style for simplicity.*
- *Using this to disadvantage operators with something to lose like our License or ReOC, I also want small FPV quads exempt as the expense to do this is not sustainable or realistic. I strongly disagree with having to keep a cellular connection, this is not achievable and will disadvantage people who make a living from this. I also don't want the costs of policing this to come down and having to be paid for by operators.*

If you had to choose between Broadcast remote ID (BRID) or network based remote ID (NRID), which do you favour?



Comments

- *the complexities of NRID are far too high.*
- *Mobile coverage is not everywhere.*
- *Broadcast is more robust, but I strongly believe in a networked environment as complementary, but it introduces more failure points which can't be assured.*
- *Connectivity issues if out of network coverage*
- *Need to know where the drone is to provide situational awareness.*
- *Privacy risk are lower, but still provides key benefit*
- *I do not have sufficient knowledge to form an opinion.*
- *No Knowledge of Either*
- *This system would allow for a nationwide approach.*
- *Because suggesting NRID in a country such as Australia must surely be a joke - the inclusion of it in the govt documentation indicates CASA cluelessness re the realities of life beyond suburbia.*
- *not sure*

- *Connection difficulties inherent in the network model*

- *The information only needs to be available for those in the vicinity*

- *NRID has been dropped in the USA for so many reasons, I can’t believe we are now proposing the same thing. This means i the operator needs an internet connection at all times, and this is not possible or cost effective and as someone who works everyday flying drones and needs a connection for instrument approvals its a huge problem, they drop out and wont connect and it’s another barrier to us making a living.*

- *LTE 4G/5G/XG coverage is not assured in AU remote areas.*

If the government decided to mandate remote ID, who should have access to the data and what information?

- *Only authorised people. Not for general access. There are a lot more safety concerns with public access to the data than from the zero deaths due to drones.*
- *It should be public.*
- *For a start - it would be whoever wants to. Gov't doesn't have a good track record of data storage!*
- *CASA.*
- *The Data should generically be available, but perhaps not all data as currently prescribed. If the data is not secured from the outset, it will by default be available to all.*
- *CASA / Police.*
- *Law enforcement to enable timely investigations and CASA to provide insight into drone use and compliance.*
- *No data should be stored. Only basic positional information should be broadcast during an operation.*
- *CASA and the individual RePL/ReOC holder.*
- *Government and approved USS providers and other service providers should have full access to the data. Beyond that, if the data is anonymised it should be publicly available.*
- *All aircraft in flight for TCAS like operations in real-time, law enforcement / regulatory services as part of an investigation (warranted) for historical data.*
- *Casa & its reps*
- *Regulators and Law Enforcement. The general public should not have access.*
- *Government aviation bodies - only.*
- *anyone using aircraft or drones.*
- *CASA data - drone ID and geographic location of use*
- *This is the key issue - data access. If the primary reason for Remote ID legislation is aviation safety, then CASA should be solely responsible for the access and processing of data.*
- *It depends what information is contained in the data.*

- *Data should be freely accessible to all.*

- *authorities or their representatives only. drone type, location, and owner.*

- *Replicate the same as ADS-B today. Why would it be treated any differently. All authorities who need access to this information today have existing processes & MOUs with CASA for this already.*

- *CASA and Airservices, the police already have the capability to track people, ive seen it in action working at events so the argument that they need this is redundant now.*

- *Industry bodies and agencies. Name and details of user.*

- *All aviation*

- *Data should be strictly limited to critical aviation operations only and only sufficient data to allow safe airspace usage and detection of illegal operations. It should never be used as a drone policing tool beyond that, ever! Currently its the genuine operators that are footing the bill and putting up with the red tape for operating within legislation, there is little or no monitoring of illegal drone activity.*

- *CASA*

- *CASA + Airservices only for ID purposes*

- *Regulator & Airservces, position, registration or ACID only, equivalent to crewed aviation standards*

- *ALL AIRSPACE USERS*

Is there any other feedback you would like to provide?

- *Remote ID needs to be conceptualised to provide solutions to industry and be an enabler, not solely an enforcement tool. The benefit needs to be for industry (and individuals/recreational operators) holistic adoption will then follow.*

- *There would need to be significant collaboration between the state and federal agencies if there was a desire to prosecute or investigate alleged offences. This would need to occur prior to implementation as requiring people to comply and not having the workforce to investigate is a nonsense.*

- *There should be strong opposition to the implementation of Remote ID just because 'someone else did it'. The burden and negative impacts it would have on ordinary non-commercial operators should not be forgotten, and there are many examples to refer to from other countries that have implemented RID requirements. If any RID was to be mandated for unmanned operations, it should be equally mandated for manned operations.*

- *Although I believe it important for authority to be able to track and identify idiots and irresponsible users I would hope authorities do not go for an overkill in this area*

- *Why should all of Australia's drone owners have RID foisted upon them when all but a handful of operations are VLOS - short, low-flying flights within a few hundred metres of the operator. If it was going to be blanket across the board - the ONLY way to do it is via retailers; mandatory owner rego at POS (point of sale). Yes there would be direct imports but these will remain a minority - most drones are bought within Aus. Certain segments of the drone industry - notably the flying taxi vulture capitalists - are pushing for tech & regs that suit their personal interests. They have way too much clout. Ditto businesses that earn a living providing Australia's too-expensive base level training/certification & BVLOS application services - etc. The advocacy for small businesses (several employees), sole proprietors & recreational flyers - which includes the upcoming generations of tech experts (kids) - is almost non-existent. Yet these are by far the majority of people involved in Australia's drone industry - tens of thousands of them; not the BVLOS flyers, drone deliverers or flying taxi spruikers - who only number in the hundreds (if that).*

- *While anything that increases safety is supported, it needs to be compulsory for all drones to be beneficial.*

- *This is a great initiative, this needs to be accelerated asap as a matter of priority. This would alleviate majority of the need around the rubbish privacy proposal put forward as it would help remove the illegal / non-compliant use.*

- *I like the idea of Remote ID but i also know what the government is like and people will find ways around this and it's my experience that people doing the right thing already are the ones that will be at a disadvantage. Please fight at the very least to remove the Network Remote ID option this can't be a solution on the table it's just not realistic in Australia.*

- *Laws are only for honest people, so like all current legislation the professional operators in the industry will be the targets and bear the cost, as dodgy operators just find their away around whatever systems are in place, and if they are not licensed or registered they are not being monitored in anyway and never get audited, they take their chances knowing there are very few resources allocated to monitoring illegal drone operations.*

- *There is little gain in spending and imposing requirements on the RPAS industry alone to solve the problem where ADS-B addresses the issues for both crewed and uncrewed operators and off the shelf mature solutions exist and may be adopted quickly, at little cost across the stakeholder groups*