Australian Government

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

EMERGING AVIATION TECHNOLOGIES

Remote Identification (Remote ID)

Discussion Paper for Public Consultation

June 2023

June 2023 / INFRASTRUCTURE 2023

Ownership of intellectual property rights in this publication

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.

Creative Commons licence

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

DOCUMENT CONTROL

Revision date	Version number	Changes made
November 2022	0.1	Initial consultation draft
December 2022	0.2	Second consultation draft (incorporation of feedback from Aviation Industry Working Group (AIWG))
April 2023	0.3	Public consultation draft (incorporation of feedback from National Emerging Aviation Technologies Consultative Committee and the Uncrewed Traffic Management (UTM) Industry Working Group)

Table of Contents

List of Figures and Tables

Introduction

Remote Identification (Remote ID or RID) is a technology incorporated into drones that can provide information about where drones are flying, and supports identifying drone operators and holding them accountable for their actions.

This paper is the first step towards a potential Remote ID mandate for drones. The paper:

- identifies opportunities and risks associated with this technology
- outlines some of the current approaches for managing these issues
- proposes an approach to policy development.

It is a starting point for ongoing discussions and collaboration between government, industry and the broader community.

This discussion will help us know how best to integrate this technology, ensuring Australia can benefit from the considerable opportunities provided by emerging aviation technologies while at the same time managing the risks and impacts associated with their use.

The consultation process will lead to developing policy options through a formal Policy Impact Analysis process during 2023.

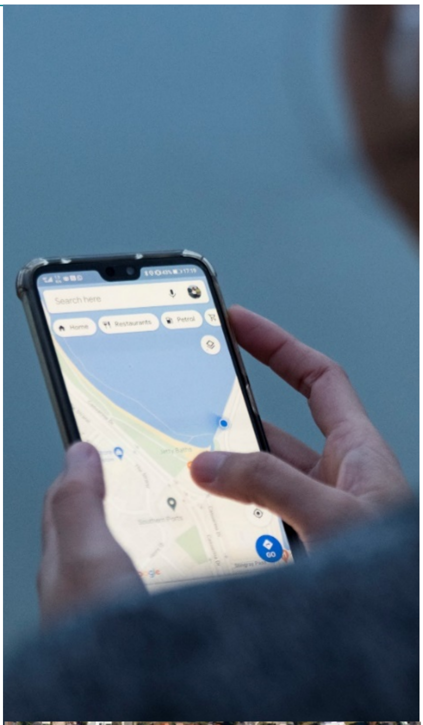
The discussion paper explores the users, uses, benefits and challenges of Remote ID, and starts the discussion by posing questions across three broad themes:

- Data and Access
- Technology
- Usage

The paper also includes three Annexes which expand on information provided in the main part of the paper and provide additional context, including technical information.

We invite feedback by Friday 28 July 2023, 17:00 AEST via www.infrastructure.gov.au/have-your-say or drones@infrastructure.gov.au.

The discussion paper has been developed by the Department of Infrastructure, Transport, Regional Development, Communications and the Arts, following targeted engagement with other government agencies and industry.



1. Purpose

Options are currently being considered for mandating Remote Identification (ID) for drones to improve safety and enable responsible and accountable drone use.

This paper is the first stage of public consultation on the potential introduction of Remote ID requirements for drones in Australia.

2. Background

While Remotely Piloted Aircraft Systems (RPAS) or Uncrewed Aerial Systems (UAS), commonly known as drones, bring many opportunities for recreational, commercial and government use, the growth in drone numbers is putting pressure on existing systems and could impact aviation and public safety if no action is taken.

We need to consider what systems or processes will be needed to manage drones into the future. This includes systems to better identify where drones are operating and who is operating them. This information will be useful for flight and public safety, airspace management, policing activities and to improve public perception of drone technologies.

As is the case with traditional aviation, better information about where aircraft are operating remains integral to the safe and efficient operation of drones. Remote ID technology is an essential step towards this. It will support security and rule compliance, and will be a critical element of future air traffic management systems (including the uncrewed traffic management (UTM) system) that will integrate crewed and uncrewed aircraft in Australian airspace.

Global harmonisation and industry collaboration will be crucial to giving the commercial drone industry certainty as it continues to grow, as well as protecting the rights of hobbyists to operate alongside commercial operators.

3. What is Remote ID?

Remote ID refers to a system that communicates flight and identifying information about a drone to other parties. Details may include:

- a unique identifier (such as a registration, serial number, or a government issued registration label)
- flight characteristics (location, altitude, speed, direction and timestamp)
- ground control station information (location and elevation)
- the type of drone and its status
- details of the owner or operator of the drone.

4. How does Remote ID work?

Types of Remote ID

There are broadly two types of Remote ID:

- Network-Based Remote Identification (NRID), or ‘standard’
- Broadcast Only Remote Identification (BRID), or ‘limited/direct’.

NRID simultaneously broadcasts drone flight data from the aircraft and transmits this to a centralised system through a network signal such as LTE, 4G, 5G or satellite. This method allows any device with connection to both the internet and the relevant network to receive this data.

BRID transmits information using a signal that can be viewed and acted on by users with the appropriate technologies in the immediate vicinity of the drone.

Drone activity data collected by either NRID or BRID can then be displayed in a visual format similar to a live aircraft flight tracking tool.

NRID and BRID each have their own benefits and challenges. See **Annex 1** for further information on each Remote ID technology type.

Standards

There are international, country and region-specific standards that cover technical aspects of Remote ID, such as:

- message formats
- transmission methods
- minimum performance requirements.

International standards include those published by the International Organization for Standardization (ISO), ASTM International and ASD-STAN. Country/region specific standards exist in the United States (US), Europe (EU), and France. See **Annex 2** for further information on international approaches and standards for Remote ID.

Australia's policy settings will need to consider when to use existing standards, and identify if and where adjustments will be needed to ensure Remote ID is fit-for-purpose for Australia's operating environment.

5. Users, uses and benefits

Remote ID **users** could include:

- drone operators and crewed aircraft users
- the Civil Aviation Safety Authority (CASA), Airservices Australia, and other Australian Government agencies
- state and territory government agencies
- members of the public.

The **uses** and **benefits** for Remote ID could include:

- Increased situational awareness to prevent mid-air collisions with traditional aircraft and other aircraft.
- Helping track illegal or noncompliant drone use and report potentially suspicious drone activity to relevant authorities for further action.
- Helping educate the community around local laws and regulations relating to drone use.
- Gathering of data which will form an evidence-base to support future regulatory and policy development.
- Facilitate faster, more efficient, and/or automated approvals to operate in airspace for which drones may need permissions.
- Support management of, and response to, other drone related issues such as noise, privacy, and environmental concerns, including through adjacent technologies such as the future UTM.

6. Challenges

To realise the benefits and utility of Remote ID, various challenges will need to be overcome. Some of these include the following:

- The costs of Remote ID:
    1. Existing drone operators would need to add Remote ID equipment to their drones.
    2. Different parts of the drone sector may be disproportionately impacted (e.g. particular drone users or types of operations).
    3. Responsible Government departments and agencies may need additional resources to develop, implement and enforce Remote ID requirements.
- The data availability will vary in different locations and contexts (e.g. urban, regional and remote), as some Remote ID technologies (such as NRID) will rely on network connectivity.
- Interoperability with other systems, including a Flight Information Management System (FIMS) and the UTM ecosystem.
- End user experience, including how information collected by Remote ID systems is presented and viewed.
- Privacy and cyber security safeguards as Remote ID systems may collect, store and transfer private, personal, and commercial information.

See **Annex 3** for more information on the uses, benefits and challenges of Remote ID.

7. Proposed Policy Options

This discussion paper seeks feedback on the potential introduction of Remote ID requirements for drones in Australia.

All options are being considered, including 'no action' or only introducing Remote ID for a subset of aircraft classes or use cases. A Remote ID mandate may be limited based on a range of factors, including:

Drone related	Location and airspace risk related
• Drone category (e.g. micro, very small, small, medium, large and excluded categories)	• Type of operation or flight authorisation (e.g. Visual Line of Sight (VLoS), Extended Visual Line of Sight (EVLoS), Beyond Visual Line of Sight (BVLoS), area approvals)
• Type of operator (e.g. commercial, recreational, government, one pilot to many drone operations)	• The quantity of operators in the same volume of airspace
• Type and complexity of operation (e.g. delivery, surveying, swarm, light show/activities)	• The location of drone operations (e.g. urban, regional, rural/remote)
• Costs (e.g. retrofitting of existing aircraft)	• Areas designated specifically for drone use (e.g. some recreational/model aircraft facilities, testing facilities, danger areas, government facilities)
	• Terrain and topography

Table 1: Some factors for consideration for Remote ID mandates in Australia.

Implementation

Implementation of Remote ID will need to consider the expected cost, size, and weight of Remote ID equipment as these characteristics will affect the incorporation of Remote ID with drones, particularly for smaller categories of drones where slight changes in weight may have a considerable impact.

As the industry continues to evolve, we will need to consider an iterative review mechanism to ensure Remote ID provisions remain fit-for-purpose.

8. Have your say

We are seeking your views on key policy considerations for successful adoption of Remote ID in Australia.

The below questions are intended to guide your feedback and responses. You may choose to respond to all or a subset of them directly, or a provide a separate response. We are also happy to receive supplementary information.

We invite feedback by Friday 28 July 2023, 17:00 AEST via www.infrastructure.gov.au/have-your-say or drones@infrastructure.gov.au. Feedback received after this date will be incorporated into the subsequent formal Policy Impact Analysis process.

Data and access questions

1. Who should have access to Remote ID data and to what information?
2. Should there be a data collection standard?
3. What is the best method of providing Remote ID data to relevant stakeholders?
4. What types of drone operators should be required to carry Remote ID equipment to operate drones? What should be exempt and why?
5. How can Remote ID privacy issues be managed?

Technology questions

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?
7. What factors should Remote ID mandates be based on, e.g. location, airspace related, other?
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?
9. What features does Remote ID require to ensure tamper resistance and to mitigate security issues (including cyber risks)?

Usage questions

10. What impacts could mandatory equipage have on drone operators?
11. Should mandatory equipage be rolled out to all drone operators, or phased through types of operators and/or operations?
12. Are there existing standards that should be considered/adopted to facilitate Remote ID uptake in Australia?
13. Who should we be engaging with, particularly outside of the aviation industry (e.g. telecommunications providers)?

9. Next Steps

Next steps will include further consultation through a Policy Impact Analysis, which follows the Australian Government's Policy Impact Analysis Framework[1].

The Policy Impact Analysis will consider:

[1] The Office of Impact Analysis, 'Australian Government's Policy Impact Analysis Framework', date cited March 2023, <www.oia.pmc.gov.au/resources/guidance-impact-analysis/australian-government-guide-policy-impact-analysis>

- Analysis of the cost and funding implications of Remote ID, including merits of NRID and BRID in various contexts and applications, as well as the relative costs of Remote ID and other options such as existing aircraft conspicuity and identification systems.
- Analysis of Remote ID legal issues, some of which may have a critical bearing on the development of a Remote ID system and the choices about what kind of arrangement may be progressed to address implementation challenges such as meeting safety, security and accountability outcomes.
- Decisions about the data to be handled by a Remote ID system including: the data to be collected and disseminated; data standards (if applicable); the protections to be afforded to that data; the other uses to which the data may be put; and the assignment of responsibility for data management[2].
- How Remote ID will integrate with and support other systems such as UTM.

The Policy Impact Analysis will define and further explore the options discussed in this paper. These will be released on the www.drones.gov.au website in 2023.

[2] Separately, the department is developing privacy guidance documentation for drone operators which will available on www.drones.gov.au. This will include information about data management in relation to drone activity.

Annex 1 – NRID, BRID and ADS-B: detailed discussion

Network Remote ID (NRID)

HOW DOES IT WORK?

NRID (depicted below in Figure 1) transmits data to other users on a closed network. Typically, LTE 4G/5G/XG is utilised to transmit this data. This method allows any device with a connection to both the internet and the relevant network (if required) to receive this data. This allows information to be dispersed between operators and systems via this network, regardless of where either the drone or the receiving device is, provided they have internet access.

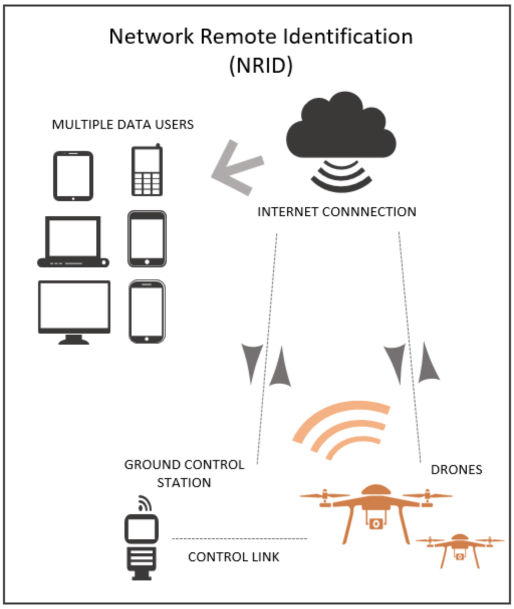


Figure 1 – Network Remote ID

ADVANTAGES

NRID provides a much wider range of visibility than BRID which can be useful for advanced drone operations such as BVLoS. NRID enables the type, and amount, of information provided to different users to be controlled and adjusted, which allows a wide range of users to access required data while maintaining appropriate levels of privacy. NRID would also support data collection and exchange between adjacent systems such as a non-safety ruleset and constraint management system, a coordinated detection and data sharing network, a national drone registration scheme, and a future UTM ecosystems, including a FIMS.

CHALLENGES

NRID's has two major challenges. Firstly, the potential cyber security and data protection concerns that come with any type of network, particularly when Remote ID interfaces with adjacent user data and air traffic management systems. Secondly, Australia has large areas with little to no network coverage, such as rural or remote areas, which would have a direct impact on the performance of NRID as current standard requirements necessitate continuous connection to a network for NRID to work. Satellite could be a bearer of NRID in these locations, however this may be cost prohibitive.

There may be additional costs associated with infrastructure to support NRID, some of which may be passed onto users of the system.

Broadcast Remote ID (BRID)

HOW DOES IT WORK?

BRID (depicted below in Figure 2) utilises equipment either built into, or retrofitted onto, a drone. This equipment then continuously transmits data to compatible receivers within a certain distance from the drone.

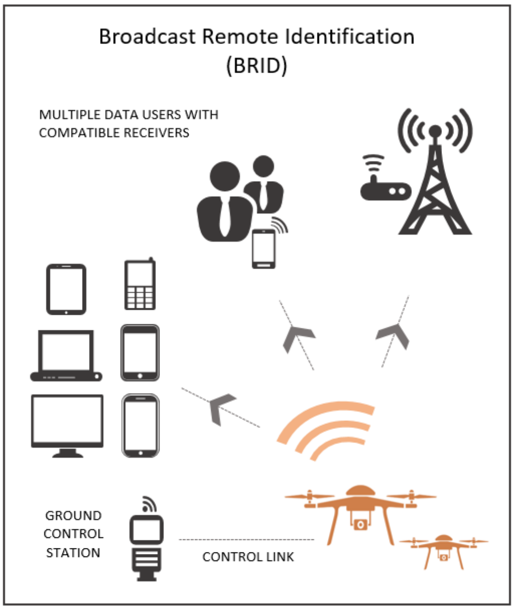


Figure 2 – Broadcast Remote ID

ADVANTAGES

BRID can be used in areas with limited network coverage via short-range wireless technologies such as Bluetooth and Wi-Fi. Due to not connecting to a network, BRID will have different cyber security and data protection issues to NRID. A data compromise risk may still exist as anyone with a suitable receiver could potentially obtain data through BRID.

Wi-Fi BRID specifically has been adopted in some countries internationally due to ease of adoption and low cost of the solution. BRID has been mandated by the Federal Aviation Administration (FAA), the US transportation agency and the European Union Aviation Safety Agency (EASA). This may offer Australia valuable insights from lessons learnt in those jurisdictions as well as benefits of scale to adopting comparable technology rather than a unique Australian implementation.

Consideration should also be given to the use of aggregated BRID, using multiple receiver stations across extended geographies and streaming the Remote ID data into an aggregated view.

CHALLENGES

Due to the nature of broadcast, drones can only be detected within a limited range. The detection range will depend on a number of factors such as the technology employed, the transmitter power, the signal frequency, and the receiver sensitivity. The detection range should be designed to support the intended application.

BRID broadcasts the identifying message to anyone with an appropriate receiver, meaning that unless that signal is shared with a network, it is only able to be seen by compatible receivers in the area. The information being broadcast can only be controlled by limiting who has access to a compatible receiver and depends on the availability of a network of BRID receiver infrastructure, with its associated costs. Limiting access to this information however, could make that information inaccessible for other airspace users and nullify its primary intention, including for outcomes related to aviation safety.

Automatic Dependent Surveillance - Broadcast (ADS-B)

Automatic Dependent Surveillance - Broadcast (ADS-B) is a surveillance technology that periodically broadcasts position estimates via on-board navigation technologies such as the Global Navigation Satellite System (GNSS).

ADS-B is not considered a suitable technology for meeting Remote ID requirements as it does not offer authentication or encryption and may have security implications. Further, the number of unique drones broadcasting using ADS-B could overwhelm the frequency bands in use and reduce the overall reliability of the system as a tool for conspicuity.

The FAA provisions prohibit the use of ADS-B OUT as a means of meeting Remote ID requirements as well as prohibiting the use of ADS-B OUT on drones unless authorised

Annex 2 – International approaches and Standards

Remote ID has been mandated by both FAA and EASA to come into effect in 2023 and 2024 respectively. There are currently two major standards being used for Remote ID:

- The US is using ASTM – F3411-19.
- The EU is using ASD-STAN – prEN 4709-002.

With a mandate from the two prominent government regulatory bodies, it is likely that most manufacturers will produce compliant hardware as standard in the coming years.

Currently, both the FAA and EASA are only mandating BRID. Some drones are exempt from this rule provided they are operating in an approved area. Under the FAA mandate, the FAA Recognised Identification Areas (FRIA) are designated areas that anyone can fly in, but can only be established by certain organisations. This gives operators exemption from the Remote ID mandate in an area that is below a determined safety threshold. EASA require all drones operating in U-Space to be equipped with NRID. U-Space is a dynamic class of airspace which is administered through a UTM system.

Both the ASTM and ASD-STAN standards being adopted by EASA and FAA outline the usage of Bluetooth or Wi-Fi for transmission due to the widespread availability of these communication protocols (including mobile phones and laptops).

Annex 3 – Uses, Benefits, Challenges and Other considerations related to Remote ID

Remote ID can be utilised to enable the complex, and increasing number of drone operations, to occur safely within Australia. Remote ID will also aid in the development of evidence and risk-based regulations and policy by providing identifying data about drones.

The intention of Remote ID is to support safe drone operations, additionally to support regulators and other Commonwealth agencies achieve compliant drone operators, identifying the drone control station and operator. It can also be used by other relevant agencies to identify non-cooperative drone activity, including when a drone appears to be flying in in an unsafe, unlawful or malicious manner or in an unauthorised location.

Uses and Benefits

MITIGATING AIRSPACE RISK

Remote ID could be used, with additional complementary systems, to identify other drones operating in the same area and provide an operator with a degree of situational awareness. Looking forward, this technology may also support integration with crewed traffic in all airspace classes, which could then support integration of Remote ID technology into the Air Traffic Management (ATM) environment in some circumstances. While the Remote ID standards outline a certain level of accuracy, it will be important to understand the accuracy of GNSS, and other relevant system, performance, as these may impact overall Remote ID accuracy.

Remote ID has the potential to be an enabling technology in Australia's regulated UTM architecture, similar to those put forward by the FAA and the National Aeronautics and Space Administration (NASA), and modelled by EASA. UTM as an ecosystem covers all airspace and associated requirements in the same way ATM considers all classes of airspace. Enabling UTM using Remote ID will require a novel approach to managing airspace traffic. It is anticipated that Remote ID will only be used for drone-to-drone separation as it is not compatible with the equipage requirements of crewed aircraft.

By providing situational awareness, Remote ID could also be used in certain contexts to strategically mitigate risk of collisions under a traditional collision risk management model used in the Specific Operations Risk Assessment (SORA) framework. However, as it is not yet a mature technology, its level of assurance would likely only facilitate effective risk mitigation for already low risk airspace operations. As this technology is better understood, its level of assurance may increase, allowing it to be an effective mitigation tool for drone use in higher risk airspace.

INFORMING POLICY AND REGULATION

The widespread use of Remote ID would enable the understanding how a drone identifying data management system works, as well as ensuring availability of useful data needed to inform policy and regulatory development relating to drones.

For policy development, Remote ID represents an integral part of drone awareness management. The use of this system, as well as the data collected by it, could inform the development of more complex and integrated tools such as: non-safety ruleset and constraint management systems; coordinated detection and data sharing networks; a FIMS; and the UTM ecosystem. Supporting these initiatives and activities, Remote ID would be foundational for understanding not only how drones can safely integrate into airspace but how security, privacy, noise and environmental issues can be managed using reliable identifying information about drones.

From a regulatory standpoint, this data could be utilised to inform the analysis of the crossover point between self-separation and the need for a managed environment, which is a key deliverable in the CASA RPAS and Advanced Air Mobility (AAM) Strategic Regulatory Roadmap. This data could also be used to provide tangible evidence to support operator applications and assessments and inform ongoing regulatory and policy development. With a goal to reduce the level of regulatory oversight and involvement in day-to-day drone operations as the industry grows in maturity and number.

COMMUNITY EDUCATION

Numerous education campaigns could be derived from the uses of Remote ID to increase awareness and understanding of drone regulations and instil positive drone operator behaviours, including a strong safety culture. This will assist to foster community acceptance and social license for drone technologies and operators.

Remote ID data could be used to inform education and promotional material by providing quantifiable evidence regarding drone operations. This data could also potentially be used to provide education about the rules for drones and target educational materials to areas and communities with increased drone usage in order to alleviate concerns about privacy, noise and environmental issues, as well as criminal and unlawful use of drones.

CONFORMANCE MONITORING

Remote ID can be used to support conformance monitoring as part of a broader UTM, in a similar way to ADS-B technology in the ATM ecosystem which utilises ADS-B to monitor compliance with flight plans and airway clearances in addition to managing aircraft separation. The aggregation of data can be used to inform the development of flight path deviation calculation (e.g. Total Systems Error), useful for separating drones from each other and to check operator and organisational compliance. Similarly, Remote ID could be used to monitor drone traffic for conformance with operational approvals, intended flight paths and filed flight plans (if required). This can aid in identification of common trends of non-conformance, which could be used to identify areas of concern and implement broader initiatives to support the sector. Remote ID may also be able to support aviation safety outcomes by directly informing ATM decisions. Other considerations, including the accuracy of track information, as well as known standards for navigational performance and separation, will need to be considered as part of a broader set of tools to effectively monitor conformance.

ENFORCEMENT

The enforcement of unlawful and criminal use of drones presents many challenges. This includes various kinds of regulatory enforcement for breaches of rules and regulations, and law enforcement for criminal offences committed using drones, up to and including prosecution.

Remote ID can be used as a tool to support the enforcement of CASA aviation safety drone rules, as well as other rules relating to security, privacy, noise and environmental issues. This would be made possible through data accessibility and other initiatives such as verification with drone registration data if the aircraft is broadcasting their details is linked to a managed registration database.

Remote ID may support the collection of data by law enforcement and other relevant authorities where, drones with Remote ID enabled, have been used to commit more serious offences, including crimes such as stalking and harassment, hostile reconnaissance, delivery of banned or illicit substances, surveillance or a kinetic attack.

Even if Remote ID has been deliberately disabled, drones are more easily identifiable when combined with other systems such as drone detection capabilities.

By supporting the linking of drones to operators, Remote ID has the potential to contribute to evidence to support enforcement actions against unlawful drone use and/or breaches of mandatory Remote ID equipage and use.

Remote ID can improve regulatory and law enforcement agencies' situational awareness of drone activities. This supports faster and more accurate responses, more accurate identification and attribution, and enables an electronic record of drone activities that can support investigations and (if necessary) further prosecution. NRID, combined with other systems, can present a technical solution that enables authorised users to consult historical information to determine whether drone activity was unlawful, including to identify patterns of behaviour.

Challenges

OBLIGATIONS ON SECTOR AND IMPLEMENTING AGENCIES

Mandatory equipage of Remote ID may have operational, procedural, administrative and/or cost implications on the emerging aviation technologies sector, and may disproportionately impact different parts of the sector. As there are already Remote ID requirements in the US and EU, some drones already have built in Remote ID capability as standard, otherwise Remote ID modules could be purchased to attach to drones. If the module is interchangeable between drones, operators who own multiple drones may have a more cost-effective option to use Remote ID.

Commercial or government users who operate a large fleet of drones or who fly frequently, depending on their operation, may be required to upgrade or retrofit equipment, update flight procedures and manuals and/or undergo further regulatory certification with resulting cost implications.

Recreational operators, or those who operate one or two Commercial Off-The-Shelf (COTS) drones, may have less equipage requirements than other operators, or may be required to operate within designated flight areas, such as Model Aircraft Association sites, when operating drones that are not Remote ID capable.

Recreational hobbyists who build and modify drones may also face disproportionate cost impacts and/or technical challenges to implement Remote ID equipage obligations.

Government and other relevant agencies will face challenges (e.g. resourcing and cost) of implementing Remote ID policies, regulations, systems, procedures and protocols into their internal systems, including to ensure that the changes brought about by Remote ID are compatible with existing settings.

INTEGRATING DRONE REGISTRATION DATA

In Australia drone registration is required if you fly a drone for a business or as part of your job. Registration for recreational drone operators may be required in the future. CASA's registration database will have significant benefits to Remote ID, enabling its smooth implementation. More information on drone registration is available on the CASA website .

Significant challenges have been faced in obtaining consistent, easily captured and enforceable information, that can identify drones for the purpose of maintaining a centralised drone registration database. This is largely due to manufacturers having varying identification methods, ranging from in-house serial number conventions, to not having a unique identifier at all.

Complicating this, there is typically no connection between an identifying feature (such as a physical serial number) and the aircraft's in-flight conspicuity. Even if a drone can be linked to a registered owner, the operator may be different, or may be an individual operating a drone registered to an entity.

To fully realise the utility of Remote ID technology, the challenge of integrating registration data, drone data and flight data will have to be overcome. Leveraging user registration data from a national registration system, and corroborating this information with Remote ID data, may enable more streamlined and accurate drone owner and operator identification. This will foster improved operator accountability (see Enforcement) while improving safety outcomes and social licence.

These changes will also work towards creating consistency when manufacturers progressively incorporate Remote ID hardware in their aircraft.

Some drone manufacturers have aligned their in-house serial number convention for aircraft manufactured from 2022 onwards, to conform to having a serial that is replicated across all locations (product box, airframe and electronic identity). These manufacturers are building new COTS drone models with Remote ID built-in as standard, using the same Remote ID identifier as the serial number.

DATA RELIABILITY

The use of NRID in Australian urban and regional centres should, in most cases, meet the minimum fidelity and latency requirements for operational outcomes. However, limitations on reliable carrier network signal across rural and remote areas in Australia means the feasibility of mandatory equipage of NRID capable drones needs to be considered carefully.

BRID may, in some cases, be able to assist where the local environment does not meet baseline NRID data reliability requirements. Additional consideration will need to be given to terrain and topography, and whether some areas should be exempted from Remote ID requirements due to the type of operations in the area, the low volume of operators and/or a low overall risk.

There are still questions as to the accuracy, integrity, availability and continuity of the data provided by Remote ID. Underlying GNSS, INS and other sensor data onboard a drone may impact the accuracy of data. The reliability of the outputs such as position and track, used for any situational awareness, may be affected and could cause issues around availability, integrity and continuity of data for its use in safety critical functions.

DATA AND SYSTEM INTEGRITY

There are multiple points in the Remote ID architecture that could present a cyber security threat. Due to transfer of data over an internet connection, NRID carries risk of data manipulation and exfiltration, as with any networked environment, these can be mitigated through device, data transfer and database security protocols.

Cyber security and data breaches present risks of system degradation or user data exposure. It also carries financial and reputational risks that can undermine community confidence in drone use and how the use of these technologies is managed by operators and relevant government authorities.

PRIVACY

Due to the nature and purpose of Remote Identification, Remote ID systems may collect, store and transfer private, personal and/or commercial information. This may include sensitive information about the drone operator, or potentially about customers using a service provided by a drone operator.

In developing Remote ID systems, relevant Commonwealth, state and territory privacy laws may apply and must be taken into consideration, particularly the Privacy Act 1988, and associated Australian Privacy Principles (APPs).

DETECT AND AVOID (DAA)

Remote ID is not considered a suitable means of DAA. Following investigations by the FAA and others, looking at Remote ID as a means of DAA, have deemed it not feasible due to the increased complexity and higher standards for latency that would be required. In all jurisdictions with Remote ID currently in place, the objective of Remote ID remains for conspicuity, accountability, enforcement and security purposes.

Other considerations

BEYOND VISUAL LINE OF SIGHT (BVLOS)

As an electronic conspicuity tool, Remote ID will improve situational awareness of drones and drone operators. This may present additional value for drone operations that are BVLoS. Remote ID has the potential to support BVLoS operations in the future by contributing to flight and identifying information, and deconfliction in conjunction with adjacent systems such as drone detection, DAA and the UTM ecosystem.

Note that the range of technologies used for NRID and BRID currently will not automatically endorse or support drone equipment or BVLoS operations directly. Investigations into policy and regulatory solutions for future applications are underway.