Submission 147 - Thales

THALES
Building a future we can all trust

274 Victoria Road
Rydalmere, NSW 2116
Australia
Tel: +61 (0)2 9848 3500
Fax: +61 (0)2 9848 3888
www.thalesgroup.com.au

4 September 2023

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

Dear Director,

Subject: Response to Emerging Aviation Technologies – Remote Identification (Remote ID) Discussion Paper for Public Consultation (June 2023).

Further to our previous submission dated 28th July 2023, Thales Australia (Thales) has reviewed the content submitted, and has revised our position regarding release of the material. As a consequence, we have removed the "Commercial in Confidence" marking, and also advise that we are happy for the released material to be attributed to Thales.

A new submission is attached, which is otherwise identical to the material previously submitted.

We look forward to continuing the discussion.

Yours Sincerely,

Philip Swadling
Technical Director, Avionics
Thales Australia

Email: philip.swadlng@thalesgroup.com.au
[redacted]

DATA AND ACCESS QUESTIONS

DATA AND ACCESS	
Question	**Response**
1. Who should have access to Remote ID data and to what information?	Remote ID data should be accessible to: • UTM service provider for unmanned traffic management purposes. • Air Navigation Service Provider (Airservices) • Aviation Safety Regulator (CASA) • Commonwealth and State law enforcement • Other government departments Members of the public should have restricted access, with data privacy taken into account. This would just be Drone Id and location. This would be analogous to the public having visibility of a car's licence plate number but not the car owner's name, or current public access to ADS-B data via apps such as FlightRadar24.
2. Should there be a data collection standard?	Data should be collected and used in accordance with the Commonwealth and State Privacy Acts. As noted in the Discussion Paper, there are several Remote ID standards (i.e. ASTM F3411-22A, ASD-STAN prEN 4709-002). These should be assessed in order to decide the best standard to adopt in Australia that provides the information required.

DATA AND ACCESS	
Question	**Response**
3. What is the best method of providing Remote ID data to relevant stakeholders?	Ideally, at least some the over the air data needs to be encrypted because data such as operator geographic location are included the Remote ID standards. The collection and distribution of BRID is more complex, as the range of the system is limited. The type of communications technology used (Bluetooth or Wifi) will enable any device within range to acquire the signal and display the information. Only authorised users would be capable of decrypting operator location data. NRID is subject to serious coverage limitations although it is the better compared to BRID for BVLOS operations. Its suitability depends on coverage the network provides over the airspace that the intended drone operations will take place. Satellite communication is best for coverage limitations but is costly and requires more complex equipment to be fitted to the drone (although this element is reducing as direct to satellite from handset capabilities are coming on to the market). Data from NRID can be gathered to a centralized cloud, and thence made available to authorised 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?	A key objective of Remote ID is improving security and making on drone operators more accountable. A second objective ID is to increase situation awareness for airspace managers and users. This can happen only when the maximum (ideally all) drones are communicating their ID and location. Drones flying in controlled airspace, engaged in any type of commercial services or in airspace where crewed flights are operating must be mandated to be fitted with Remote ID. Drones registered for display or recreational purposes with permit from the local council for the event granted prior to the event could be exempted. Some exceptions could be drones operating in agricultural use-cases or operations in areas with very sparse population. Also in special cases, for example where a drone is tethered. Potentially Drones registered for display purpose in a specific area with permit from the local council or other authority for the event granted prior to the event could be exempted. (Geocaging capability should be a requirement for this type of exemption). Smaller recreational drones only flown in defined locations could also be exempted.

DATA AND ACCESS	
Question	**Response**
	It is suggested that subsidies such as the current CASA subsidy for ADS-B, be considered to maximise take up of Remote ID, especially among non-mandated drones.
5. How can Remote ID privacy issues be managed?	Stakeholders should have different levels of data access: For example: 1. Members of the public should only be able to see the unique identifier and drone location (not operator location) 2. Airspace management authorities should have full access to all the information 3. Law enforcement should have full access to all information 4. Other authorities should be able to access data following authorisation based on need The ability to implement these access constraints is dependent on the technology being used.

TECHNOLOGY QUESTIONS

Technology	
Question	**Response**
6. Is Remote ID (BRID, NRID or both) an appropriate solution for Australia? Are different types of Remote ID more fit-for-purpose in different contexts or applications? Are there other types (or variations of types) of Remote ID that should be considered?	For simple VLOS flight in controlled airspace BRID seems the most relevant because of its low cost and ease of implementation. When it comes to BVLOS or more complex operations, Network Remote ID provides a better capability as it is only limited by Network coverage. Furthermore, if it's connected to a centralised cloud, all the relevant stakeholders can have access to the data.
7. What factors should Remote ID mandates be based on, e.g. location, airspace related, other?	Remote ID mandates should be based on the type and complexity of operations, considering factors such as: • Location • VLOS or BVLOS • Controlled airspace or not • Operational risk (e.g. weight of the drone)
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?	We suggest to adopt a harmonized standard with ASTM (U.S) and EUROCAE (EU) so that there is one standard industrial implementation of Remote ID to deploy anywhere in the world. This will allow the manufacturers to deploy drones, and operators to provide services easily across the world. Adopting a standardised integration API protocol method to UTM to have a harmonised way to supply tracking information to all UTMs around the world is also important. We recommend using an event subscription protocol is recommended to provide better performance when tracking traffic at scale.

<table>
<tr><th colspan="2">Technology</th></tr>
<tr><th>Question</th><th>Response</th></tr>
<tr><td>9. What features does Remote ID require to ensure tamper resistance and to mitigate security issues (including cyber risks)?</td><td>A Some important cyber features in the embedded device as well as cloud services to be considered to reduce cyber risk:
- All data exchange between Remote ID on board UAV to any ground systems should be encrypted end to end with mutual authentication to provide confidentiality as well as to protect against spoofing
- Unique digital keys and certificates per device to reduce the risk of mass cyber-attack on the devices
- Short lived keys and certificates to renew the lifecycle (preferably not more than 2 years)
- Digital keys and certificates life cycle renewal after expiration
- Digital keys and certificates to be stored in tamper proof device such as embedded SIM
- Digital keys and certificates revocation capability to identify and remove the compromised devices from the ecosystem.
As noted above, drone Id and location may not be encrypted if public access is to be provided.</td></tr>
</table>

USAGE QUESTIONS

Usage	
Question	**Response**
10. What impacts could mandatory equipage have on drone operators?	Operators will have to adapt their platform to integrate Remote ID on it, driving cost. Use of NRID could add mobile data subscription costs as well. Add on Remote ID units can be made very small and self-contained, so except for the smaller there would be minimal impact on performance. Fully integrated units would have even less performance impact. In exchange, Operators will be able to reduce administration time to get authorisation to fly in zones they were not able to access before, and will have a centralized platform where they can track all their flights in real time.
11. Should mandatory equipage be rolled out to all drone operators, or phased through types of operators and/or operations?	As discussed in response to question 7 above, Remote ID requirements could be different depending on the nature of the operations. BVLOS operators should move directly to Network Remote ID when VLOS operators can start with BRID for less complex operations before moving to NRID for operations in controlled airspace.
12. Are there existing standards that should be considered/adopted to facilitate Remote ID uptake in Australia?	ASTM standard F3411 could be adopted to be harmonised with other regions. EUROCAE is also referencing ASTM standards to formulate an industry standard for EU region. FAA 14 CFR Part 89 has rules and specification for the USA. EU Remote ID rule is ASD-STAN DRI It will be worthwhile trying to understand both FAA rule (stated above) and EU rule on Remote ID came into force in 2020 and understand the differences and if the standards provide means of compliance to the rules.

Usage	
Question	**Response**
	FAA Part 89 defines the ruling of compliance with broadcast Remote ID to operate drone weighing more than 250g. F3596 defines the standard practice, test steps, passing criteria to be compliant with Part 89. ASD-STAN prEN4709-002 provides means of compliance with the "Direct Remote Identification" requirements set in Regulation (EU) 2019/945 on Unmanned Aircraft Systems.
13. Who should we be engaging with, particularly outside of the aviation industry (e.g. telecommunications providers)?	It is assumed here that the aviation industry is considered to include traditional crewed aircraft stakeholders (including equipment and systems providers such as Thales), as well as drone manufacturers and operators, CASA and Airservices. Telecommunication providers are very important partners and stakeholders of Network Remote ID to provide good data signal coverage in the sky. Other suggested stakeholders include: • Law enforcement agencies • Privacy Commissioners • Local Councils • Other state and federal departments and agencies, such as National Parks • Major infrastructure operators • Users of drone services

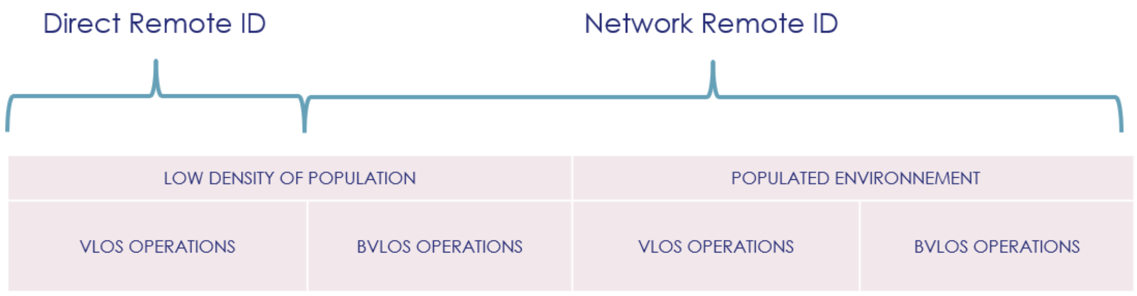
ADDITIONAL INFORMATION

COMPARISON OF NRID AND BRID CHARACTERISTICS IN KEY AREAS

Below is a summary of the operational behaviour of both Broadcast Remote ID and Network Remote ID based on a few key characteristics.

Characteristic	Broadcast Remote ID	Network Remote ID
Range	Direct RID is **short range** (max 1.0km theoretically depending on the wireless technology used) from the drone to the ground receiver with line of sight	Network Remote ID is **Long Range**. Coverage depends on the Cell Tower availability & height / directivity of the RF Antennas.
Data Reliability & Security	BT / WiFi are **open** wireless systems - signal reliability depends on the congestion in the **local RF environment** and the quality of ground receiver (a public smartphone may not always be reliable – dedicated ground receivers are possible but will increase the cost drastically).	Cellular signals are associated with a **Quality of Service** – there is higher accountability on signal reliability than open wireless systems. Signal Availability Maps are also available by Cellular Service Providers over a specific route or area of operation. **Higher level of security** is possible on Cellular networks with GSM standards like **IoT Safe.**
Future Scalability	**Suitable for VLOS operations** because of Direct Remote ID's limited range. If Direct Remote ID is to be used for BVLOS, a dedicated ground sensor network would be necessary which is untenable for a nationwide implementation	**Suitable for BVLOS operations.** Authorities can remotely monitor & track drones (crucial for nationwide monitoring) with Network Remote ID.
Cost	The cost of implementing Direct Remote ID on the drone is minimal. However, for a reliable implementation an extensive sensor network will be required which would drive bigger cost of the ground infrastructure	The Remote ID standard is driven by **IoT principles**, which means the bandwidth / data requirement is actually quite low. Example ~ a few **100 MB's of data** per month is sufficient for a drone operation – high value for the cost.

OPERATIONAL SCENARIOS FOR DIRECT / NETWORK REMOTE ID



Direct Remote ID is adapted to less complex operations and it is a low-cost solution to enforce accountability. **Network Remote ID** is adapted to more complex operations with no limit of range (within coverage constraints) to adapt to BVLOS operations. Hence, it helps to ensure compliancy and accountability at any time of the operations with real time data provided to airspace authority and operators.

REMOTE IDENTIFICATION AROUND THE WORLD

Region/Country	Regulation
EU	Broadcast Remote Identification for SAIL I and SAIL II operations Network Remote Identification for SAIL III operations and above
US	Drone users to be compliant with Broadcast Remote Identification starting Sept 2023
Japan	Drone users to be compliant with Broadcast Remote Identification
Singapore	Drone users to be compliant with Network Remote Identification with local standards

RECOMMENDATIONS

- There is an increasing trend of deployment of IoT devices globally as well as in Australia. This means that telecommunications providers will continue to invest in enhancing the network coverage to diversify and increase their revenue stream. With the reasonable and growing coverage of mobile/IoT data coverage in Australia, the drone industry should leverage this to support BVLOS operations. There also significant effort in securing IoT data traffic, which could also be leveraged.
- Network Remote ID by itself doesn't require a high data bandwidth & data consumption – which would keep the cost of connectivity quite low
- Network Remote ID is best suited to match Australia's vision of large scale, high-value drone operations envisioned in the coming years. Direct Remote ID is still applicable for current VLOS operations and in less complex scenarios.