Submission: 078

Ross Farrell

While ADS-B remains the cornerstone of crewed aviation surveillance, mandating its adoption for uncrewed aircraft systems (UAS) is neither technically appropriate nor operationally sustainable. Instead, Australia should adopt a Remote ID–based surveillance model tailored to the unique requirements, scale, and risk profile of the emerging uncrewed aviation sector.

Position Statement

While ADS-B remains the cornerstone of crewed aviation surveillance, mandating its adoption for uncrewed aircraft systems (UAS) is neither technically appropriate nor operationally sustainable. Instead, Australia should adopt a Remote ID–based surveillance model tailored to the unique requirements, scale, and risk profile of the emerging uncrewed aviation sector.

1. Spectrum Management and Network Congestion

ADS-B operates on 1090 MHz—a finite frequency already congested by high-density airspace operations. Extending continuous ADS-B transmissions to hundreds of thousands of small UAS would:

Overload the 1090 MHz spectrum, degrading signal integrity for safety-critical crewed operations.

Increase collision risks through signal interference and message saturation, particularly in metropolitan areas or during emergency response deployments.

Undermine ICAO spectrum efficiency standards, which explicitly discourage non-critical use of the ADS-B channel.

Remote ID, by contrast, uses Wi-Fi/Bluetooth Low Energy broadcast or cellular-based network delivery, providing scalable, localized identification without burdening safety-critical frequencies.

2. Proportionality and Risk-Based Regulation

ADS-B was designed for aircraft with significant kinetic energy, extended range, and high-altitude flight profiles. Applying that same requirement to low-altitude UAS:

Violates proportionality principles in risk-based regulation, as sub-2 kg drones flying below 400 ft pose fundamentally different hazards.

Imposes unnecessary hardware and certification costs—many times the value of the aircraft—creating inequitable barriers for small operators, innovators, and educational users.

Diverts safety investment away from actual risk mitigation (e.g. geo-fencing, detect-and-avoid algorithms) into avionics compliance.

Remote ID achieves equivalent safety and accountability outcomes for the risk class, enabling identification, accountability, and enforcement without excessive cost or technical overreach.

3. Privacy, Security, and Operational Data Management

Continuous ADS-B transmission exposes detailed telemetry (position, velocity, ID) to the public domain—creating:

Cyber-security vulnerabilities for operators and infrastructure assets.

Privacy concerns for operators in sensitive industries (defence contractors, surveyors, utilities).

Data governance conflicts under Australia's Privacy Act and forthcoming digital identity legislation.

Remote ID supports privacy-aware architectures—data can be selectively broadcast (for local awareness) or securely shared via encrypted network layers accessible to CASA and law enforcement. This achieves accountability without universal public traceability.

4. Infrastructure and Cost Efficiency

ADS-B requires certified avionics, antennas, and continuous GNSS transmission—components often exceeding the payload capacity or economic rationale of small UAS.
Conversely:

Remote ID modules are low-power, low-cost, and software-definable, with many consumer drones already equipped via firmware.

Remote ID infrastructure leverages existing telecommunications networks and consumer devices as receivers, minimizing the need for government-funded ground stations.

This approach supports rapid national adoption and progressive integration into the broader Unified Traffic Management (UTM) ecosystem without expensive retrofitting or airframe redesign.

5. Interoperability with Emerging Airspace Systems

The future of Australian airspace management will depend on network-centric, layered surveillance—not monolithic broadcast systems.
Remote ID is:

Interoperable with UTM standards (ASTM F3411, EUROCAE ED-282, ICAO RPAS CONOPS).

Easily upgradable to integrate with 5G-based Network Remote ID, data fusion, and dynamic airspace management platforms.

Aligned with international best practice: both the FAA (USA) and EASA (EU) have adopted Remote ID rather than mandating ADS-B for UAS, specifically citing scalability and spectrum protection.

ADS-B's rigid broadcast architecture is ill-suited to the evolving digital ecosystem of automated flight corridors, swarm operations, and beyond-visual-line-of-sight (BVLOS) systems.

6. Policy Alignment and Innovation Enablement

By embracing Remote ID as the default identification layer, Australia would:

Maintain consistency with international regulatory trajectories (FAA, EASA, ICAO).

Encourage domestic innovation in UAS manufacturing, Remote ID chipsets, and networked flight management systems.

Position itself for seamless cross-border integration and participation in global drone logistics and emergency-response frameworks.

This approach aligns with the 2024 Aviation White Paper's goal of safe, scalable, and innovative airspace management while preserving the integrity of ADS-B for its intended users—manned aviation.

Conclusion

Expanding ADS-B to uncrewed systems would be a technical regression—solving yesterday's surveillance problems with yesterday's tools.
Remote ID, in contrast, provides a fit-for-purpose, scalable, and secure identification system that aligns with modern risk management, protects critical frequencies, and fosters innovation across the UAS ecosystem.

Australia should therefore adopt a Remote ID–based compliance framework as the cornerstone of uncrewed aircraft surveillance, reserving ADS-B for its intended role within traditional air traffic management.