



AUSTRALIAN
AIRPORTS
ASSOCIATION

HOME AFFAIRS

DRONES SECURITY PUBLIC CONSULTATION PAPER – APRIL 2026

AUSTRALIAN AIRPORTS ASSOCIATION (AAA)



CONTENTS

Overview	1
1. Proactive management of emerging drone threats	1
2. Strengthened counter-drone capabilities	2
3. Enhanced drone identification and tracking	4
4. Balanced enforcement that deters misuse and supports innovation	5
5. Drone classifications and operating restrictions	6
6. Public and industry awareness	7
Conclusion	7

ACKNOWLEDGEMENT OF COUNTRY

The AAA respectfully acknowledges the enduring connection of the Traditional Owners to the lands and waters across Australia.

We extend our respect to the wisdom and guidance of elders, both past and present. In sharing our narratives, we recognise that the Aboriginal and Torres Strait Islander peoples are the original custodians and storytellers of their ancestral homelands.

Overview

The Australian Airports Association (AAA) represents more than 340 Australian airports and aerodromes, from local community airstrips to major international gateways. This submission focuses on reforms that will help Australian airports manage drone-related safety and security risks while preserving legitimate drone use for inspection, emergency response, mapping and other productive activities.

The AAA supports a modern, risk-based framework that aligns with aviation safety regulation and gives airports practical tools to protect runways, approach and departure paths, navigation aids and other critical airport assets. International airport disruptions, including Gatwick and the recent European incidents referred to in the Consultation Paper, show that even a small number of drones can disrupt aviation operations and public confidence.¹²

1. Proactive management of emerging drone threats

Question (Consultation Paper): Are there specific risks you believe are unique to maritime or land-based drones that should be addressed differently within a national framework?

For Australian airports, aerial drones are the immediate priority. They are widely available, fast moving and able to enter airport operating areas in ways that traditional perimeter controls cannot manage. The framework should therefore deal with aerial drones first while remaining flexible enough to cover land and maritime systems where they affect airport operations.

Land and maritime systems can still create airport-specific risks. Larger airports are increasingly using or trialling autonomous airside ground equipment, inspection robots and ground vehicles. Coastal and island airports may also be affected by maritime drones near approach paths, navigation aids or offshore restricted areas. Surface and underwater devices can be harder to detect than aerial intruders, and hybrid systems could launch aerial drones close to a coastal airport. Any changes to airside vehicle or aviation security rules should be evidence-based, risk-based and developed with the airport sector.

Question (Consultation Paper): How can a mode-agnostic, technology-neutral framework ensure legitimate commercial and recreational users are not unduly burdened while still mitigating security risks?

A mode-agnostic framework should set outcome-based security obligations rather than prescribe particular technologies. Obligations should scale by risk, including operating location, drone weight, payload, capability and activity type. This would let airports, contractors and legitimate drone operators adopt solutions suited to their operating environment without imposing unnecessary compliance costs.

¹ The December 2018 drone incursion at London Gatwick resulted in the cancellation of approximately 1,000 flights and disruption to more than 140,000 passengers and is identified in the Consultation Paper as a catalyst for Australia's initial regulatory response.

² Drones Security Public Consultation Paper, April 2026, Department of Home Affairs, p. 10 (Case study: European Union Counter-drone policy development).

For airports, the framework should align with CASR Part 101, the Aviation Transport Security Act 2004 and CASR Part 139, and should build on CASA-supported passive surveillance trials, CASA-verified drone safety apps and the Automated Airspace Authorisations Trial.³⁴⁵ The national framework should not replace airport detection and perimeter security work already underway; it should make those initiatives easier to use consistently across major city and regional airports.

Question (Consultation Paper): Are there sectors that may face disproportionate impact from an all-modes approach, and how should government address these impacts?

Regional airports may face disproportionate costs from new requirements. Many operate with limited staff and resources while supporting regular passenger transport, freight, medical flights, emergency response and community connectivity. A single model for all airports could impose costs and complexity that are not proportionate to the risk at smaller airports.

The Government should design scalable obligations based on airport size, traffic profile and operational risk. It should also consider shared services, pooled detection capability and implementation funding so regional airports can access appropriate support without each airport having to buy and maintain its own full counter-drone system.

2. Strengthened counter-drone capabilities

Question (Consultation Paper): What safeguards or oversight do you think are important to ensure counter-drone technologies are used safely, proportionately, and appropriately?

The AAA supports stronger counter-drone arrangements where they are safe, proportionate and clearly authorised. Airport operators and vetted contractors should be able to use passive detection and identification technology. Active mitigation, including jamming, spoofing or kinetic measures, should remain with authorised police and security agencies operating under agreed airport response protocols. This approach is consistent with the layered airport protection model promoted by Airports Council International, which emphasises detection, identification, tracking and legally authorised mitigation supported by clear protocols between airports, air navigation service providers and security agencies.⁶

Legislation should state who may use each capability, when it may be used and what oversight applies. Equipment used near airports should meet aviation safety, ACMA radiocommunications and cybersecurity standards. Operators should be trained and accredited, with deployment logs and data-handling records available for oversight. Pre-deployment risk assessments are essential near airports because poorly controlled counter-drone measures could interfere with GNSS, navigation aids, communications or aircraft systems.

³ Civil Aviation Safety Authority, passive drone surveillance trials at major mainland capital city aerodromes (focused on airport boundaries and approach/departure paths) and at Sydney Harbour, conducted from 2018 onwards.

⁴ Aviation Transport Security Act 2004 (Cth); Civil Aviation Safety Regulations 1998 (Cth), Part 139 (Aerodromes) and Part 101 (Unmanned aircraft and rockets).

⁵ Civil Aviation Safety Authority and Airservices Australia, Automated Airspace Authorisations Trial (extended to November 2026), covering Adelaide, Broome, Cairns, Canberra, Coffs Harbour, Essendon, Hobart, Melbourne, Perth and Sydney airports, and Sydney Harbour Restricted Areas R405A/B.

⁶ Airports Council International (ACI) World, Counter Drone Systems and Airport Drone Protection policy resources, aci.aero.

Privacy and proportionality should be built in through data minimisation, retention limits and access controls. Where possible, non-destructive measures such as triggering return-to-home or directing a controlled landing should be preferred over measures that could create debris, leave an unsecured device in the operating environment or allow a third party to recover and reuse the drone.

Question (Consultation Paper): Who should be authorised (with appropriate training and approvals) to deploy drone detection or counter-drone technologies?

Authorisations should draw a clear line between detection and mitigation. Passive detection and identification should be available to approved airport operators and their vetted, accredited service providers, as well as other critical infrastructure operators where the risk profile supports it. Access should be subject to licensing, training, technical standards, privacy obligations and reporting requirements.

Active mitigation should remain with properly authorised police and security agencies. Those agencies should operate under protocols agreed in advance with airport operators, CASA, Airservices Australia and, where relevant, Defence, so they can respond quickly at both major and regional airports without role confusion or duplication.⁷

Question (Consultation Paper): What concerns do you have with expanded or additional counter-drone measures being introduced for authorised groups in Australia?

The AAA's main concerns are aviation safety, equipment integrity, liability, operational coordination and cost. Radiofrequency interference with GNSS, communications, navigation aids or aircraft systems is the most immediate safety concern. Detection or counter-drone equipment used near airports should come from trusted vendors and meet Australian technical and cybersecurity standards.

Liability should be settled before incidents occur, including responsibility for secondary harm if mitigation causes a drone to crash. Roles between airport operators, CASA, Airservices Australia, police and security agencies must be agreed before a live incident. New measures should also preserve airport detection and perimeter security trials already underway and should not impose unfunded technology mandates on regional airports.

Question (Consultation Paper): What role should industry and the public play in reporting or helping to identify emerging drone threats?

Airport operators, airlines, ground handlers, tenants and local communities are often the first to see unusual drone activity around airports. The AAA supports a single, simple reporting channel for security-related drone incidents at airports, aligned with existing CASA, ATSB and aviation security reporting to avoid duplication.

Information should flow both ways. Airports that report incidents should receive feedback, and agencies should share timely information during live events. A public reporting option, including anonymous reporting of suspected misuse, would be useful if supported by clear messaging

⁷ Department of Defence, LAND 156 Counter Small Uncrewed Aerial Systems (CsUAS) Standing Offer Panel, established January 2026

that drone misuse near airports is taken seriously. Manufacturers and retailers can also help by embedding reporting prompts in drone safety apps and point-of-sale material.

3. Enhanced drone identification and tracking

Question (Consultation Paper): What level of real-time visibility (e.g., location, altitude, or operator attribution) should authorities have to detect, track and identify drones operating near sensitive or high-risk environments?

Near airports and other high-risk locations, authorities should have real-time visibility of a drone's 3D position, speed and direction of travel, the operator's identity linked to registration, the operator's physical location and the flight authorisation status where relevant. This information helps agencies distinguish authorised activity from careless or hostile activity and helps airports avoid unnecessarily conservative operational responses.

Access should be tiered. Detailed operator information should be available to police and security agencies. Airport security teams should have access where it is operationally necessary to manage aviation safety or security. All access should be subject to privacy, audit and data retention safeguards.

Question (Consultation Paper): Should drone detection equipment only be available to police and security agencies, or extended to new user groups such as emergency services, prison operators, critical infrastructure operators and event organisers?

Detection equipment should be available beyond police and security agencies where the risk justifies it. Airport operators, prison operators, emergency services, critical infrastructure operators and major event organisers should be able to deploy passive detection under an approval or licensing framework. For airports, this should include training, accreditation, technical standards that prevent interference with aviation systems, privacy obligations and information-sharing requirements with police, CASA, Airservices Australia and other relevant agencies.

CASA's passive surveillance trials around capital city airports show that detection near airports is technically useful and operationally relevant. Active mitigation should remain with properly authorised agencies under agreed protocols. Airports will also need clear visibility of expected response times for those agencies actively countering drone threats which is critical information required for airports deploying complimentary security and safety measures.

Question (Consultation Paper): Currently only aerial drones used for commercial purposes must be registered. What drones should be subject to registration or other forms of enhanced identification requirements?

The AAA supports expanding registration and electronic identification in a proportionate way. Australia should continue to register all commercial drones and should also register recreational

drones above a sensible weight threshold, such as 250 grams, consistent with international practice in the United States and European Union.⁸⁹

Registration should attach to operators as well as devices so the responsible person can be identified. Authorised entities should be able to query the national register in near real time, subject to appropriate safeguards. The Government should also consider requiring operators to authenticate against their registration in the drone's operating software before flight, linking each flight to an identifiable person rather than only to a device.

Question (Consultation Paper): What other enhanced identification and electronic conspicuity technologies are available that could support security outcomes?

A mix of technologies will provide the best airport coverage. Broadcast Remote ID, network Remote ID, passive radiofrequency detection, radar and acoustic detection each have a role. Radar and acoustic systems are particularly relevant for drones that emit weak or no ordinary control signals, including modified or fibre-optic controlled drones.

Integration with Airservices Australia's future Flight Information Management System will be important as new airspace users increase around airports.¹⁰ CASA-verified drone safety apps could also embed operator credentials and digital licences so approvals, restrictions and identity information are easier to verify before and during flight. ADS-B should be used cautiously for drones, given spectrum congestion and aviation safety considerations.

4. Balanced enforcement that deters misuse and supports innovation

Question (Consultation Paper): What penalties or consequences would most effectively deter unauthorised or unsafe drone operations near sensitive locations while remaining fair and proportionate?

Current penalties for breaches of CASR Part 101 are reported to be about \$1,000 to \$1,500 per offence, which is too low to deter deliberate or repeated incursions near airports where disruption can be severe.¹¹

The AAA recommends graduated enforcement. Accidental, lower-risk breaches should be addressed through education, warnings and infringement notices. Repeated or reckless breaches should attract higher civil penalties, equipment seizure and suspension or cancellation of approvals. The most serious conduct, including deliberate interference with aircraft, weaponising drones, contraband delivery or conduct linked to organised crime or terrorism, should attract criminal penalties. Penalties for incursions near aerodromes and other

⁸ Federal Aviation Administration, Remote Identification of Unmanned Aircraft, 14 CFR Part 89. Full operator compliance required from 16 March 2024.

⁹ European Union Aviation Safety Agency, Commission Implementing Regulation (EU) 2019/947 on the rules and procedures for the operation of unmanned aircraft, and Commission Delegated Regulation (EU) 2019/945 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems.

¹⁰ Airservices Australia, Flight Information Management System (FIMS), under development to support integration of new airspace users including drones and Advanced Air Mobility.

¹¹ Civil Aviation Safety Authority enforcement reporting; recent penalties for breaches of CASR Part 101 reported in the order of \$1,000 to \$1,500 per offence.

sensitive airport assets should be higher than the general baseline and easy for recreational and commercial users to understand before they fly.

Question (Consultation Paper): What reporting obligations should apply when abnormal or unauthorised drone activity is detected (e.g., mandatory incident reporting by infrastructure operators), and how should information be shared with authorities?

The AAA supports mandatory reporting of significant abnormal or unauthorised drone activity by airport operators, provided reporting is aligned with existing aviation safety and aviation security obligations. Clear thresholds should define what must be reported so reports focus on useful safety and security information.

A single national reporting channel should share information between Home Affairs, CASA, ATSB, Airservices Australia and police and security agencies. Airports that report incidents should receive feedback so they can improve local response arrangements and share lessons across the sector.

5. Drone classifications and operating restrictions

Question (Consultation Paper): Should specific no-use or enhanced-monitoring zones be designated around certain assets (e.g., hospitals, correctional and energy facilities)?

Yes. For airports, designated zones should include permanent restrictions around movement areas, approach and departure paths, control towers, navigation aids, fuel facilities and other infrastructure critical to aviation safety or security. Enhanced monitoring zones should also be considered around airport precincts, where drone activity may be permitted with prior approval but should be visible to airport operators and authorities.

Temporary restrictions should be available for emergencies, VIP movements, major events and other short-term airport risks. Risk-based arrangements should also apply to non-controlled certified aerodromes that support regular passenger transport, medical services or other essential services.

Question (Consultation Paper): What areas should be completely restricted from drone operations (unless approved)?

In the airport context, complete restrictions should apply to movement areas, including runways, taxiways and aprons, approach and departure path corridors with appropriate vertical and lateral buffers, airside operational zones, and zones around infrastructure critical to safety or security. Approval pathways must remain available for legitimate airport inspections, emergency response, maintenance and contracted work, ideally through existing CASA approval channels and the Automated Airspace Authorisations Trial.

Question (Consultation Paper): How should 'no-drone-zones', or enhanced-monitoring zones be communicated, including to ensure proper coordination between enforcement entities and authorised operators?

Clear digital maps integrated into CASA-verified drone safety apps would have wide reach. Geofencing of restricted and enhanced-monitoring zones should be built into drones sold or imported into Australia, with reliable automatic updates from manufacturers. Tightening import

regulations should be considered as part of this process, which given the challenges of stopping non-compliant devices, should commence as soon as possible.

Airport operators, CASA, Airservices Australia, police and security agencies should agree coordination protocols and shared data feeds before incidents occur. Physical signage in publicly accessible areas near airports also has a role, particularly for casual recreational users and visitors. Over time, integration with Airservices Australia's Flight Information Management System should support consistent automated communication of restrictions.

6. Public and industry awareness

Question (Consultation Paper): What information would help the public better understand risks associated with drones across land, air, and maritime domains?

Public information should be simple, visual and airport-specific where relevant. It should explain where drones can and cannot be flown, why incursions near runways and approach paths are dangerous, how to report concerns and what penalties apply. Maps, infographics and short videos usually have appeal for a wide audience.

Question (Consultation Paper): What communication channels or resources would make it easiest for operators to understand their responsibilities under a future all-modes framework?

Communication should use channels drone users already use: point-of-sale material, packaging warnings, manufacturer apps, CASA-verified drone safety apps, hobby clubs, training providers, model aircraft associations and drone courses. These channels are especially important for new or casual users who may not know about airport restrictions.

Airports can support awareness through signage, websites, traveller communications and engagement with local communities, contractors and airport tenants. Airlines can help international travellers understand Australian drone rules.

Question (Consultation Paper): What public communication or education would help recreational and commercial operators avoid entering restricted airspace and understand their responsibilities?

The AAA recommends a sustained government-led campaign with consistent messaging, real-time maps of restricted zones and temporary changes, and targeted local education where new restrictions apply. Messaging should emphasise that responsible drone use protects aviation safety and supports legitimate drone services.

Conclusion

The AAA supports the direction of the Consultation Paper and would welcome continued engagement on airport-specific detection, regional airports, incident reporting and integration with aviation safety and security regulation. The final framework should build on existing airport, CASA and Airservices Australia initiatives, give airports practical detection and reporting tools, and keep active mitigation with authorised agencies. Early consultation and engagement with sector during the design phase of any legislation, particularly where it directly impacts their operations, would be very welcome.



AUSTRALIAN
AIRPORTS
ASSOCIATION

AUSTRALIAN AIRPORTS ASSOCIATION (AAA)

Level 1, 55 Blackall Street, Barton ACT 2600

P: 02 6230 1110

E: info@airports.asn.au

W: www.airports.asn.au