Submission to the Department of Home Affairs

PROPOSED APPROACHES TO AUSTRALIA'S DRONE SECURITY

Submitted by: Steve Griffin, Uncrewed Approvals
Consultation: Drones Security Public Consultation Paper, April 2026
Date: 25 May 2026

1. Introduction

Uncrewed Approvals welcomes the opportunity to respond to the Department of Home Affairs consultation on proposed approaches to Australia's drone security framework.

Australia needs a stronger and more modern drone security framework. The current regulatory model has largely developed around aviation safety, airspace integration and operational compliance. That has been useful, but it does not fully address the security risks now emerging around critical infrastructure, correctional facilities, major events, sensitive sites, public gatherings and government facilities. The consultation paper correctly identifies that Australia's current framework does not effectively support responses to drone-related security risks, particularly outside traditional aviation safety settings.

At the same time, drone technology is now a normal and valuable part of Australian industry. Drones support agriculture, emergency services, infrastructure inspection, mining, mapping, media, environmental monitoring and a growing range of public-sector operations. The consultation paper recognises these economic, environmental, industrial and social benefits.

The policy challenge is therefore not whether Australia should strengthen drone security. It should. The question is how to do it without damaging legitimate, compliant and beneficial drone operations.

Uncrewed Approvals supports a national, risk-based drone security framework that:

- targets actual security risk rather than treating all drone use as suspicious;
- distinguishes between authorised, negligent, reckless and malicious activity;
- gives authorised agencies practical powers to detect, identify and respond to genuine threats;
- protects compliant ReOC holders, trained remote pilots and legitimate commercial operators;
- avoids creating unnecessary barriers for low-risk drone operations;
- improves education and public awareness;
- supports national consistency rather than a fragmented patchwork of localised restrictions.

The Aviation White Paper already recognises that drones and other new aviation technologies will increasingly share airspace with conventional aircraft, and that policy and regulatory approaches must adapt to capture benefits while managing risk. The drone security reforms should build on that approach, not sit beside it as a disconnected security overlay.

2. Overall position

Uncrewed Approvals supports the introduction of drone security legislation before 2030, provided the legislation is practical, nationally consistent and proportionate.

The Aviation White Paper committed the Australian Government to consider new legislation by 2030 to protect communities, infrastructure and businesses from security risks associated with drones and Advanced Air Mobility. The Department's consultation paper now provides an

important opportunity to shape that legislation in a way that works for both security agencies and legitimate industry.

Our central submission is that Australia should avoid a blanket-restriction model. A framework built mainly around “no drone zones”, broad prohibitions and reactive enforcement would be too blunt. It would be difficult to enforce, could restrict legitimate public benefit operations, and may not stop malicious actors who are already willing to break the rules.

Instead, Australia should adopt a layered model based on:

1. **Identification** – knowing which drones are operating, who is responsible, and whether they are authorised.
2. **Authorisation** – allowing legitimate operators to access restricted or monitored environments through clear approval pathways.
3. **Detection and response** – giving trained and authorised agencies the ability to identify, assess and respond to genuine threats.
4. **Risk-based restrictions** – applying tighter controls where the consequences of misuse are genuinely higher.
5. **Education and enforcement** – helping well-meaning operators comply, while applying strong consequences to reckless or malicious misuse.

This would better support security outcomes while preserving the growth of the legitimate RPAS industry.

3. Proactive management of emerging drone threats

Uncrewed Approvals supports a proactive national framework for drone security. The consultation paper correctly notes that drones are accessible, capable, hard to detect, hard to attribute, dual-use and rapidly evolving. These characteristics create a genuine security challenge.

However, the framework should remain grounded in operational risk. A small recreational drone flown by an uninformed operator near a sensitive site is not the same risk as a deliberately modified aircraft used for contraband delivery, surveillance, disruption or attack. The law should recognise that difference.

Australia should adopt a tiered risk model that considers:

- the location of the operation;
- the intent of the operator;
- the capability of the drone;
- the payload or sensor fitted;
- the degree of autonomy;
- whether the drone is identifiable;
- whether the operator is authorised;

- the likely consequence of misuse.

Security regulation should not be designed only around aircraft weight. Weight remains relevant for safety, but security risk may arise from payload, sensor capability, autonomy, operating location, communications links, data handling and operator intent.

A sub-250 g drone can still create a security risk if used for surveillance, reconnaissance or interference near a sensitive facility. Conversely, a larger aircraft operated by a trained and approved ReOC holder under documented procedures may present a lower overall risk than a small unregistered aircraft operated anonymously near a critical asset.

Recommendation

Australia should adopt a tiered drone security risk framework that assesses location, operator authorisation, payload, capability, autonomy, intent and consequence, rather than relying mainly on aircraft size or broad location-based restrictions.

4. Counter-drone capabilities

Uncrewed Approvals supports expanding counter-drone capabilities for properly authorised agencies and infrastructure operators, but only with strong controls.

The consultation paper correctly notes that counter-drone systems can create their own risks. Active RF-based systems may interfere with Wi-Fi, mobile networks, GNSS, aviation navigation aids and aircraft systems if not properly managed. That risk is particularly important around airports, ports, stadiums and dense urban areas.

Counter-drone powers should therefore be limited to authorised, trained and accountable parties. These powers should not be made generally available to private businesses, event organisers or members of the public without a clear approval framework.

A sensible model would include different levels of authorisation:

Detection-only capability should be available more broadly to critical infrastructure operators, major event operators, airports, correctional facilities and other approved entities. Detection systems that do not interfere with aircraft, communications or navigation systems should be encouraged.

Identification and tracking capability should be available to authorised operators where there is a clear security need and appropriate privacy controls.

Active mitigation or interdiction capability should be restricted to police, defence, national security agencies or specially authorised persons operating under strict conditions.

Counter-drone actions should be subject to:

- clear legal authority;
- documented operating procedures;
- trained personnel;
- defined activation thresholds;
- record keeping;

- post-incident reporting;
- oversight and audit;
- coordination with CASA, Airservices, police and other relevant agencies where required.

Recommendation

Counter-drone legislation should separate detection, identification, tracking and active mitigation. Detection should be enabled more broadly for approved high-risk sites, while active mitigation should remain restricted to specially authorised and trained entities under strict oversight.

5. Electronic conspicuity, Remote ID and identification

Uncrewed Approvals strongly supports improved electronic identification and tracking of drones, but it must be implemented carefully.

Remote identification is one of the most practical ways to separate legitimate operators from unauthorised or suspicious activity. It would allow police, security agencies, infrastructure operators and event managers to quickly determine whether a drone is likely to be authorised.

However, electronic conspicuity should not become an unreasonable burden for low-risk operators or a barrier to entry for small businesses.

A risk-based approach should apply. Mandatory electronic identification should be prioritised for:

- operations near controlled aerodromes;
- operations near critical infrastructure;
- operations near major events;
- operations in enhanced monitoring zones;
- BVLOS and EVLOS operations;
- higher-risk commercial operations;
- operations under specific approvals or authorisations.

For very low-risk recreational or excluded-category operations, implementation should be staged and supported by simple, affordable technology.

The system must also protect legitimate operators. Public display of pilot identity or precise personal information should be avoided. Enforcement agencies may need access to operator identity, but the general public should not be able to identify a pilot's home address, contact details or business-sensitive client information from a drone broadcast.

Recommendation

Australia should implement Remote ID or electronic conspicuity through a staged, risk-based model. The framework should support enforcement and security outcomes without publicly exposing personal or commercially sensitive operator information.

6. Balanced enforcement

Uncrewed Approvals supports stronger penalties for serious drone misuse. The current enforcement model does not always provide an adequate deterrent, particularly for reckless or malicious activity.

The consultation paper asks what penalties would deter unauthorised or unsafe drone operations near sensitive locations while remaining fair and proportionate. The answer should depend on conduct and consequence.

A tiered enforcement model should distinguish between:

1. **Unintentional or low-risk non-compliance**
   Example: a recreational operator enters a monitoring zone without understanding the requirement.
   Preferred response: education, warning, direction to land, infringement if repeated.

2. **Negligent or reckless non-compliance**
   Example: operating near a major event, hospital, emergency operation or critical facility without authorisation.
   Preferred response: infringement, aircraft seizure where appropriate, licence or accreditation consequences, possible prosecution.

3. **Deliberate or malicious misuse**
   Example: contraband delivery, surveillance of sensitive sites, interference with emergency services, disruption of transport infrastructure, hostile reconnaissance or payload delivery.
   Preferred response: criminal penalties, seizure, forfeiture, banning orders and strong interagency response.

4. **Misuse by approved operators**
   Example: a commercial operator knowingly breaches approval conditions in a sensitive environment.
   Preferred response: regulatory action against the operator and responsible persons, including ReOC consequences where applicable.

This model would protect well-meaning operators from disproportionate punishment while creating meaningful deterrence for deliberate misuse.

Recommendation

Drone security legislation should introduce a tiered enforcement model that distinguishes between accidental, negligent, reckless and malicious conduct. Strong penalties should be reserved for deliberate misuse, repeat offending, operations near sensitive sites and conduct that creates actual security or public safety risk.

7. Drone classifications and operating restrictions

Uncrewed Approvals supports restricted areas and enhanced monitoring zones around genuinely sensitive sites. However, restrictions should be specific, risk-based and supported by approval pathways for legitimate operations.

The consultation paper identifies possible higher-risk locations, including critical infrastructure, correctional centres, hospitals, government and research buildings, major events, ports, rail corridors and transport hubs. These are sensible categories for consideration.

However, not all facilities within those categories present the same risk. A small regional hospital, a major trauma hospital with helicopter operations, a correctional facility, a power station, and a temporary major event all have different risk profiles.

The framework should therefore include:

- permanent prohibited zones only where there is a strong and ongoing security case;
- restricted zones where approved operations can occur under conditions;
- enhanced monitoring zones where operations are allowed but must be identifiable;
- temporary restriction zones for major events, emergency incidents and security operations;
- clear approval pathways for ReOC holders and government operators;
- digital publication of all zones in a machine-readable format.

It is important that approved operators can still conduct legitimate work. Critical infrastructure, ports, rail, energy, telecommunications, hospitals and government agencies often need drone services for inspection, mapping, maintenance, emergency management, security and media purposes.

A "no-use unless approved" model may be appropriate in some locations, but the approval process must be fast, clear and nationally consistent. Otherwise, restrictions will slow legitimate operations while doing little to deter malicious actors.

Recommendation

Australia should adopt a three-level restricted area model: prohibited zones, restricted-with-approval zones and enhanced monitoring zones. All zones should be digitally published, nationally consistent and supported by practical approval pathways for legitimate operators.

8. Interaction with CASA and aviation safety regulation

Drone security reform must not duplicate or conflict with CASA's aviation safety framework.

The Aviation White Paper notes that CASA and Airservices are already progressing work on drone safety, airspace integration and controlled airspace access. Home Affairs should therefore focus on security outcomes, while CASA remains responsible for aviation safety.

There will need to be close coordination between:

- Home Affairs;
- CASA;
- Airservices Australia;

- police;
- defence;
- state and territory governments;
- critical infrastructure regulators;
- airport operators;
- approved RPAS operators.

The framework should clearly separate:

- aviation safety permissions;
- airspace permissions;
- security permissions;
- landholder or site permissions;
- privacy and surveillance obligations.

One of the recurring problems in the RPAS sector is regulatory overlap and confusion. Drone operators often face multiple approval pathways, unclear jurisdictional boundaries and inconsistent advice between agencies. Drone security reform should reduce that problem, not add to it.

Recommendation

The new drone security framework should include a clear interagency responsibility map so operators and enforcement agencies understand which agency controls safety, airspace, security, privacy, restricted areas and enforcement decisions.

9. Public and industry awareness

Education must be a central part of the reform.

The consultation paper correctly identifies that better education can reduce accidental misuse, prevent security incidents and build public confidence. This is especially important because many drone incidents are not malicious. They occur because operators do not understand the rules, rely on incomplete apps, misunderstand airspace, or assume that because a drone can physically fly somewhere, it is lawful to do so.

Public education should be practical and plain English. It should not be limited to general statements such as “do not fly near airports”. Operators need clear guidance on:

- where restrictions apply;
- how to check restricted zones;
- what enhanced monitoring means;
- when approval is required;
- how to obtain approval;

- what to do if approached by police or security;
- what penalties apply for serious misuse;
- how to report suspicious drone activity.

Education should also be targeted. A single generic campaign will not be enough. Different material should be developed for:

- recreational users;
- excluded-category operators;
- RePL holders;
- ReOC holders;
- critical infrastructure operators;
- event organisers;
- police and local enforcement agencies;
- local councils;
- schools and community groups;
- drone retailers.

Drone retailers and online marketplaces should have some responsibility to provide basic rule information at the point of sale.

Recommendation

Home Affairs should work with CASA, industry bodies, training providers and retailers to produce nationally consistent, plain-English drone security guidance, including digital restricted-area tools and targeted education for different operator groups.

10. Reporting obligations and information sharing

Uncrewed Approvals supports improved reporting of abnormal or unauthorised drone activity, particularly around critical infrastructure, correctional facilities, airports, emergency incidents and major events.

However, reporting obligations should be proportionate. A small business should not be required to report every harmless drone sighting. Mandatory reporting should apply where there is a genuine security concern, such as:

- repeated drone activity near a sensitive site;
- drone activity during a major event;
- drone activity near emergency operations;
- suspected surveillance of critical infrastructure;
- suspected contraband delivery;

- drone activity in a prohibited or restricted zone;
- drone activity that causes operational disruption;
- drone activity that appears coordinated, autonomous or deliberately concealed.

Reports should go to a single national reporting pathway or an agreed state/territory pathway that feeds into a national system. Fragmented reporting will reduce the quality of intelligence and make trend analysis difficult.

Recommendation

Australia should establish a single national drone security reporting pathway, supported by clear thresholds for mandatory reporting by critical infrastructure operators and other high-risk site operators.

11. Cyber and supply chain security

The consultation paper appropriately identifies that drones are connected cyber-physical systems and that cyber risks should form part of the drone security framework.

This is an important issue, but it must be handled carefully. Cyber and supply-chain risk should not be used to impose broad, unsupported bans on particular operators or technologies without a clear evidence base. However, government, defence, police, emergency services and critical infrastructure operators should be required to consider:

- data storage location;
- cloud connectivity;
- firmware management;
- command and control link security;
- payload data handling;
- manufacturer support arrangements;
- software update integrity;
- remote access risks;
- vulnerability reporting;
- lifecycle management.

For higher-risk government or critical infrastructure operations, procurement policies should include drone cyber-security requirements.

Recommendation

Cyber and supply-chain risk should be integrated into drone security reform, with stronger requirements for government and critical infrastructure use, while avoiding broad restrictions on ordinary low-risk commercial operations unless supported by clear risk evidence.

12. Protecting legitimate industry

The legitimate RPAS industry should be treated as part of the solution.

ReOC holders, trained remote pilots and professional operators already operate within documented procedures, risk assessments, pilot training systems, maintenance systems, incident reporting processes and CASA oversight. These operators can assist government by normalising accountable drone use and helping distinguish authorised operations from suspicious activity.

The reform should not create a system where compliant operators are burdened with more paperwork while non-compliant or malicious users continue to operate anonymously.

Professional operators should benefit from:

- faster approval pathways;
- recognition of ReOC systems and procedures;
- trusted operator arrangements for sensitive sites;
- digital authorisation tools;
- integration with Remote ID;
- clear points of contact for restricted-area approvals;
- ability to pre-register recurring work near sensitive infrastructure.

Recommendation

Home Affairs should develop a trusted operator pathway for ReOC holders and other approved entities conducting legitimate operations near restricted or enhanced monitoring zones.

13. Key recommendations

Uncrewed Approvals recommends that the Department of Home Affairs:

1. Introduce drone security legislation before 2030, consistent with the Aviation White Paper commitment.
2. Use a risk-based model that considers location, operator authorisation, payload, capability, autonomy, intent and consequence.
3. Avoid blanket restrictions that unnecessarily constrain legitimate drone operations.
4. Implement Remote ID or electronic conspicuity through a staged, risk-based approach.
5. Protect personal and commercially sensitive information in any identification system.
6. Separate counter-drone powers into detection, identification, tracking and active mitigation.
7. Restrict active counter-drone mitigation to properly authorised and trained entities.
8. Create prohibited zones, restricted-with-approval zones and enhanced monitoring zones.

9. Digitally publish all restricted and monitored zones in a machine-readable format.
10. Provide clear approval pathways for ReOC holders, government operators and critical infrastructure service providers.
11. Establish a tiered enforcement model for accidental, negligent, reckless and malicious conduct.
12. Create a single national drone security reporting pathway.
13. Integrate cyber and supply-chain risk requirements for government and critical infrastructure operations.
14. Develop plain-English public and industry education with CASA, industry and training providers.
15. Create a trusted operator pathway for professional and accountable RPAS operators.

14. Conclusion

Australia needs stronger drone security settings, but those settings must be practical, proportionate and risk-based.

The greatest risk is not legitimate drone use. The greater risk is anonymous, reckless or malicious drone use in locations where consequences are high and response options are unclear.

A well-designed framework should make it easier to identify legitimate operators, faster to detect and respond to genuine threats, and harder for malicious actors to exploit gaps in the system. It should also preserve the benefits that drones already deliver across agriculture, infrastructure, emergency services, public safety, mapping, media, research and regional Australia.

The Department's proposed reform direction is broadly supported. The final framework should now focus on practical implementation, national consistency, clear enforcement powers, digital tools, industry education and approval pathways that recognise professional operators as part of Australia's drone security solution.