# Submission to the Department of Home Affairs

### Consultation on proposed approaches to Australia's drone security

## 1. Introduction

I make this submission in my personal capacity.

I support the Australian Government's objective of strengthening Australia's drone security framework. Drones provide substantial economic, social, public-safety, emergency-management, agricultural, industrial, research, creative and recreational benefits. They should not be treated only as threats. However, drones are also increasingly capable, accessible, networked and difficult to attribute which means they can be misused for surveillance, interference with critical infrastructure, smuggling, disruption of emergency services, hostile reconnaissance, contraband delivery, cyber-enabled data collection and, in the most serious cases, weaponised attacks.

The Drone Security Public Consultation Paper 2026 correctly recognises that Australia's current framework has largely focused on aviation safety and integration into controlled airspace while security risks around critical infrastructure, major events, crowded places and sensitive sites require more explicit attention (Department of Home Affairs, 2026a).

My submission focuses on one core proposition; Australia should strengthen drone security through a risk-based, technically precise and privacy-preserving framework that protects high-risk places and activities without unnecessarily burdening legitimate commercial, government, research, emergency-service and recreational drone use.

## 2. Core position

Australia's drone security framework should be built around the following principles:

- risk-tiered controls, rather than blanket restrictions;
- stronger protection for high-risk places, including airports, correctional facilities, defence sites, critical infrastructure, crowded places, major events, ports, hospitals and emergency operations;
- proportionate authorisation for counter-drone capabilities;
- electronic conspicuity and identification where justified, with privacy safeguards;
- clear distinction between detection, identification, tracking, mitigation and enforcement;
- careful governance of drone detection data and operator information;
- technology-neutral rules that can adapt across aerial, land and maritime drones;
- protection for legitimate innovation and lawful recreational use;
- cyber and supply-chain security requirements for higher-risk drone ecosystems;
- clear public education, practical maps and predictable operating rules.

The framework should not create a general-purpose surveillance system for ordinary drone users. It should create focused capability to identify and respond to negligent, unsafe, criminal or malicious drone activity, especially in higher-risk environments.

## 3. Risk-tiered controls should be the centre of the framework

The consultation paper proposes a risk-based approach to drone classifications and operating areas, including permanent “no go” zones, restricted zones, enhanced monitoring zones and temporary restrictions during special circumstances (Department of Home Affairs, 2026a). That is the correct direction.

A one-size-fits-all model would be poor policy. The risk posed by a small recreational drone in a low-risk rural area is not the same as the risk posed by a drone near an airport, prison, defence site, hospital heliport, energy facility, port, emergency operation, major public event or crowded place.

The framework should classify restrictions by:

- location sensitivity;
- event sensitivity;
- airspace and operational risk;
- payload capability;
- autonomy and range;
- drone size, kinetic risk and speed;
- whether the drone can operate beyond visual line of sight;
- whether it carries cameras, LIDAR, microphones, wireless capture equipment, delivery mechanisms or other payloads;
- whether the operation is recreational, commercial, emergency-service, research, government or hostile;
- whether the operator is identifiable and authorised.

The strongest controls should apply where the consequences of misuse are highest. Low-risk users should be guided into compliance through clear rules, education, warnings and accessible tools before punitive enforcement is used.

## 4. A mode-agnostic framework is sensible, but implementation should be phased

The consultation paper proposes a sector-agnostic and technology-neutral framework initially focused on aerial drones while considering land and maritime drones over time (Department of Home Affairs, 2026a). That is sensible because aerial, land and maritime drones share important security properties; remote operation, autonomy, sensors, command links, software, navigation systems and potential dual use.

However, the framework should be implemented in phases. Aerial drones should remain the first focus because they are the most accessible, common and immediately disruptive. Land and maritime drone rules should not be copied directly from aerial drone rules without considering domain-specific differences.

Land-based drones may raise different risks around road corridors, industrial sites, pedestrian areas, mines, farms, warehouses, campuses, rail environments and private property. Maritime and sub-surface drones may raise risks around ports, undersea cables, ship movements, offshore energy, water infrastructure, defence facilities and environmental monitoring.

The framework should therefore be mode-agnostic at the level of principles but mode-specific at the level of operational rules.

## 5. Counter-drone capability should be authorised, logged and proportionate

I support expanding access to appropriate counter-drone tools for authorised agencies and high-risk operators where necessary. The consultation paper correctly identifies that counter-drone responses may need real-time detection, tracking and mitigation, and that some counter-drone capabilities manipulate the electromagnetic spectrum, including RF and GNSS interference (Department of Home Affairs, 2026a).

These capabilities are sensitive. If misused, they can interfere with Wi-Fi, mobile networks, GNSS, aviation navigation aids, aircraft systems and other critical communications. Physical interdiction can also create collision, property damage and injury risks. For that reason, counter-drone powers should be treated as operational security powers, not ordinary commercial tools.

The framework should distinguish between:

- passive detection, such as radar, optical, acoustic, RF detection and sensor fusion;
- identification and tracking;
- operator location;
- active RF or GNSS interference;
- protocol-level takeover or command interruption;
- physical interception;
- kinetic or directed-energy mitigation.

Passive detection may be appropriate for a wider set of operators, including critical infrastructure owners, event organisers, airports, ports and correctional facilities, subject to privacy and data controls. Active mitigation should be restricted to properly authorised, trained and accountable entities.

At minimum, active counter-drone powers should require:

- statutory authority or clear lawful basis;
- operator accreditation and training;
- defined use thresholds;
- safety assessment before deployment;
- logging of each deployment;
- post-incident review;
- reporting of unintended interference or safety effects;
- retention and review of operational records;
- independent oversight where powers are used by government agencies;
- strict limits on private use of RF-interference tools.

## 6. Authorisation should depend on capability type and risk environment

The consultation paper asks who should be authorised to deploy drone detection or counter-drone technologies. The answer should depend on the intrusiveness and risk of the capability.

I recommend a tiered authorisation model:

- **Tier 1: Passive awareness and reporting**
  Available to a broad set of users, including the public, drone operators, hobby groups, venue operators and businesses. This includes reporting suspicious drone activity, checking restricted-area maps and receiving public safety alerts.

- **Tier 2: Passive detection**
  Available to trained and approved operators in higher-risk environments, including airports, correctional centres, critical infrastructure operators, major event organisers, ports, emergency services and relevant government agencies. This should be subject to data-handling controls and technical standards.

- **Tier 3: Identification and operator attribution**
  Available to vetted entities with a clear need, such as law enforcement, aviation safety bodies, national security agencies, authorised airport operators, correctional authorities and selected critical infrastructure operators. Access to personal operator information should be limited and auditable.

- **Tier 4: Active mitigation**
  Reserved for law enforcement, national security agencies, authorised aviation/security bodies and tightly approved operators in exceptional high-risk environments. This should require clear legal authority, training, operational controls and post-use reporting.

This model would improve drone security while avoiding unnecessary distribution of intrusive or safety-sensitive capabilities.

## 7. Electronic conspicuity should be privacy-preserving

The consultation paper identifies enhanced identification and electronic conspicuity as a way to improve operational visibility, accountability, incident response and risk analysis while minimising burden on compliant operators (Department of Home Affairs, 2026a). That objective is valid. Authorities cannot respond effectively to unknown drone activity near sensitive sites if they cannot identify the drone, its operator or its authorisation status.

However, electronic conspicuity should not become public real-time tracking of ordinary drone operators. Broadcasting personally identifying operator information to anyone nearby may create risks of stalking, harassment, doxxing, theft of equipment, vigilantism or targeted interference with lawful operators.

The framework should separate:

- public safety information;
- authorised-security information;
- operator personal information;
- enforcement information.

For low-risk environments, public broadcast information should generally be limited to operationally necessary information such as drone identifier, location, altitude and status without exposing the operator's name, address, phone number or other personal details. Personal operator information should be available only to authorised entities under defined conditions.

Where possible, the system should use pseudonymous or rotating identifiers that allow authorised attribution when necessary but do not allow general public tracking of individuals over time. Access to attribution data should be logged, purpose-limited and reviewable.

## 8. Drone detection data should be governed as sensitive operational data

The consultation paper contemplates sharing drone detection data between government, commercial and private entities to support real-time responses to misuse with appropriate safeguards (Department of Home Affairs, 2026a). This is operationally understandable but it creates a major governance challenge.

Drone detection data can reveal:

- operator identity or pseudonymous identifiers;
- operator location;
- drone flight paths;
- facility surveillance boundaries;
- patterns of security patrols;
- event security posture;
- critical infrastructure layouts;
- incident response patterns;
- legitimate commercial activity;
- emergency-service operations.

The framework should treat drone detection and attribution data as sensitive operational data. Data sharing should be governed by:

- purpose limitation;
- role-based access control;
- need-to-know principles;
- retention limits;
- audit logs;
- onward-disclosure restrictions;
- clear thresholds for law-enforcement access;
- breach notification obligations;
- aggregation or de-identification where possible;
- public transparency about categories of data collected and shared.

The Office of the Australian Information Commissioner's guidance on APP 3 states that agencies may collect personal information only where it is reasonably necessary for, or directly

related to, agency functions or activities, and organisations may collect personal information only where reasonably necessary for their functions or activities (OAIC, 2019). That principle should shape drone detection data policy. Collect what is needed to protect high-risk environments and enforce the law, not more.

## 9. Privacy should not be treated as outside the security design

The consultation paper notes that drone-related privacy and noise impacts concern some members of the community, but says specific consideration of those matters falls outside the scope of the consultation (Department of Home Affairs, 2026a). I understand the need to keep the consultation focused. However, privacy cannot be entirely separated from drone security because several proposed security measures involve detection, identification, tracking, attribution, data sharing and operator monitoring.

The point is not that privacy should block security reform. The point is that security reform should be privacy-engineered from the beginning.

The framework should require:

- data minimisation;
- access controls;
- limited retention;
- secure storage;
- clear collection notices where practical;
- auditability;
- internal misuse controls;
- public transparency;
- privacy impact assessments for high-risk data-sharing schemes.

APP 11 requires entities to take active measures to ensure the security of personal information and to consider whether personal information may be retained (OAIC, 2025). Drone security systems should be designed with the same discipline. Detection and attribution data should not become a loosely governed operational dataset.

## 10. Counter-drone and detection vendors should meet security standards

Drone security will depend heavily on vendors; detection platforms, RF sensors, radar, optical systems, acoustic sensors, command-and-control software, cloud dashboards, mapping tools, incident platforms, identification systems and counter-drone equipment.

This creates cyber and supply-chain risk. The consultation paper recognises that drones are complex connected cyber systems, that core components such as navigation, communications, software and payload systems may be vulnerable to interference or takeover and that some countries may compel companies to provide data, systems access or technical assistance in support of state objectives (Department of Home Affairs, 2026a).

The same logic applies to counter-drone and detection systems. If a detection system around a port, stadium, prison or energy facility is compromised, the attacker may learn the site’s

security posture, blind the operator, create false positives, suppress real detections or access sensitive operational information.

The framework should require appropriate security standards for counter-drone vendors and systems, including:

- secure software development practices;
- vulnerability disclosure processes;
- signed firmware and software updates;
- update provenance and rollback protections;
- strong authentication and role-based access;
- audit logging;
- network segmentation;
- encryption in transit and at rest;
- data location and access controls;
- restrictions on support access;
- supply-chain risk assessments;
- incident notification duties;
- independent testing for high-risk deployments.

For high-risk sites, counter-drone systems should be treated as security-critical infrastructure, not ordinary surveillance equipment.

## 11. False positives and misattribution require safeguards

Drone detection is not perfect. Radar, RF detection, acoustic sensors, optical systems and sensor-fusion platforms may produce false positives, false negatives or misclassification. A detection system may misidentify birds, aircraft, environmental noise, Wi-Fi devices, reflections, benign drones or unrelated RF activity. Operator attribution may also be uncertain.

The enforcement framework should therefore require confidence thresholds before serious action is taken. Detection alone should not automatically lead to punitive enforcement unless supported by sufficient evidence especially where the result affects a person’s licence, business, employment, criminal exposure or ability to operate.

The framework should include:

- confidence scoring;
- evidence preservation standards;
- human review for significant enforcement action;
- ability to challenge or correct attribution errors;
- clear evidentiary rules for enforcement;
- post-incident review where active mitigation is used;
- public reporting on false-positive and complaint trends.

A strong framework must be technically realistic about detection limitations.

## 12. Enforcement should be tiered and focused on harm, intent and repetition

The consultation paper proposes a tiered enforcement approach, including warnings, administrative penalties or infringement notices for lower-level or accidental breaches and stronger penalties for repeated negligence, reckless operations, contraband delivery, weaponisation, organised crime or terrorism-linked activity (Department of Home Affairs, 2026a). I support that general model.

The framework should distinguish between:

- accidental or low-risk non-compliance;
- careless operation;
- repeated negligent operation;
- reckless operation;
- intentional breach of restricted areas;
- interference with emergency services;
- surveillance of sensitive sites;
- contraband delivery;
- cyber compromise or unauthorised takeover;
- organised crime use;
- terrorism or violent extremist use;
- weaponisation.

For ordinary users, education, warnings and clear compliance pathways should be preferred where there is no serious harm, intent, repetition or aggravating factor. Stronger penalties should be reserved for deliberate, reckless, repeated or harmful conduct.

This would deter misuse without making ordinary recreational or commercial users afraid of disproportionate punishment for honest mistakes.

## 13. Restricted areas should be clear, accessible and machine-readable

The consultation paper discusses permanent “no go” zones, restricted zones, enhanced monitoring zones, temporary restrictions and mandating digital rules built into devices and updated automatically such as geofenced areas (Department of Home Affairs, 2026a).

These measures are useful only if operators can understand them. Restricted area rules should be:

- publicly accessible;
- current;
- clear to non-experts;
- available through maps;
- available in machine-readable formats;
- integrated with flight-planning tools where possible;
- updated quickly for temporary restrictions;
- capable of showing reasons for restrictions at a useful level of detail;
- designed with exceptions for authorised operators, emergency services and approved commercial activity.

A person should not need specialist aviation knowledge to understand whether a simple recreational flight is lawful in a particular location. The easier it is to comply, the easier it is to focus enforcement on genuine misuse.

## 14. Geofencing should assist compliance, not become an opaque control layer

Device-level geofencing can reduce accidental misuse, especially near airports, prisons, emergency incidents, major events and critical infrastructure. However, geofencing also has risks.

If geofencing databases are inaccurate, stale, overbroad or opaque, lawful operators may be blocked without explanation. Emergency, media, research, inspection, agricultural or authorised infrastructure users may be affected. If geofencing is controlled primarily by vendors, public law may be indirectly enforced through private technical systems without enough transparency.

The framework should ensure that geofencing:

- reflects legally valid restrictions;
- is updated quickly;
- allows authorised exceptions;
- provides clear user-facing reasons for refusal;
- allows appeal or correction where boundaries are wrong;
- avoids overbroad restrictions;
- is not the sole source of legal truth;
- does not create unnecessary vendor lock-in.

Digital rules should support compliance, not replace accountable lawmaking.

## 15. Public and industry education should be practical, not abstract

The consultation paper correctly recognises that education and awareness can reduce accidental misuse, improve compliance, and help authorities focus on genuinely unsafe or unlawful behaviour (Department of Home Affairs, 2026a).

Education should focus on practical behaviour:

- how to check whether a flight is allowed;
- what to do near airports, heliports and hospitals;
- what to do near emergency operations;
- what major events and temporary restrictions mean;
- what critical infrastructure restrictions mean;
- how to interpret “no go”, restricted and enhanced monitoring zones;
- how to report suspicious drone activity;
- how to identify official information sources;
- what penalties apply to serious misuse;
- how to seek authorisation for legitimate commercial or research use.

Public communication should use multiple channels:

- drone retailers;
- manufacturers;
- firmware/app prompts;
- hobby groups;
- schools and universities;
- local councils;
- event organisers;
- aviation and model aircraft groups;
- industry associations;
- emergency-service messaging;
- plain-English government websites;
- maps and mobile-friendly tools.

Education should be designed to reduce accidental misuse before enforcement becomes necessary.

## 16. Critical infrastructure engagement should use existing trusted channels

The Trusted Information Sharing Network is the primary way for industry and all levels of government to work together to strengthen the security and resilience of critical infrastructure, including through risk identification, addressing security gaps and informing future policy and programmes (Cyber and Infrastructure Security Centre, 2026).

Drone security should use that channel. Critical infrastructure owners and operators are likely to have practical insight into site-specific risks, detection requirements, false-positive issues, data-sharing needs and counter-drone deployment constraints.

The framework should use the TISN and sector groups to develop sector-specific drone security guidance for:

- energy;
- water;
- telecommunications;
- transport;
- ports;
- hospitals and health precincts;
- food and grocery logistics;
- data centres;
- government facilities;
- major events and crowded places.

Sector guidance should be more specific than general national rules but still aligned to common principles.

## 17. Incident reporting should be standardised

The consultation paper asks what reporting obligations should apply when abnormal or unauthorised drone activity is detected. I recommend a tiered reporting model.

Mandatory reporting should apply to high-risk entities where drone activity may affect public safety, critical infrastructure, aviation, emergency operations, correctional facilities, national security or major public events. Lower-risk entities and the general public should have simple voluntary reporting channels.

Incident reports should capture:

- date and time;
- location;
- drone type if known;
- observed behaviour;
- suspected payload if visible;
- flight direction and altitude if known;
- whether the operator was identified;
- whether the drone entered a restricted or monitored zone;
- whether operations were disrupted;
- whether counter-drone action was taken;
- whether law enforcement was notified;
- supporting evidence such as photographs, video or sensor data.

Reports should feed into trend analysis, not only enforcement. Aggregated reporting could help identify emerging patterns, high-risk locations, repeated misuse and education gaps.

## 18. Public transparency should accompany stronger powers

Any expansion of drone detection, tracking, counter-drone or enforcement powers should be accompanied by public transparency reporting.

Annual or periodic public reporting could include:

- number of reported drone security incidents;
- incident categories;
- number of counter-drone deployments;
- number of active mitigations used;
- number of unintended interference or safety incidents;
- enforcement outcomes by category;
- warnings versus penalties;
- number of complaints;
- number of confirmed false positives or misattributions;
- number of requests for operator attribution data;
- categories of entities authorised to use detection or mitigation tools.

This reporting can be aggregated and de-identified where necessary. The purpose is not to reveal sensitive security methods. The purpose is to maintain public confidence that expanded powers are being used proportionately.

## 19. Innovation should be protected through predictable rules

Drone technology has legitimate and valuable uses in agriculture, mining, emergency services, environmental monitoring, logistics, infrastructure inspection, media, film, research, telecommunications, surveying and public safety. The Aviation White Paper sets out a long-term vision for Australia's aviation sector to remain safe, competitive, productive and sustainable, including enabling new aviation technologies (Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, 2024).

Security reform should support that objective. Predictable rules help responsible operators invest, train staff, insure operations and design compliant systems. Unclear or overbroad rules discourage innovation and create unnecessary compliance risk.

The framework should therefore provide:

- clear approval pathways for legitimate high-risk operations;
- transparent criteria for exemptions and authorisations;
- proportional obligations based on risk;
- predictable restricted-area data;
- reasonable transition periods;
- consultation with affected sectors;
- support for Australian counter-drone and drone-security industry development.

Security and innovation are not opposites. Good security rules can increase public trust and make legitimate drone adoption more durable.

## 20. Recommendations

I recommend that the Australian Government:

1. Adopt a risk-tiered drone security framework, with strongest controls around high-risk places, events, infrastructure and activities.
2. Implement mode-agnostic principles but phase implementation and develop mode-specific rules for aerial, land, surface maritime and sub-surface drones.
3. Distinguish clearly between passive detection, identification, operator attribution, active mitigation and enforcement.
4. Restrict active counter-drone mitigation capabilities to properly authorised, trained and accountable entities.
5. Require logging, safety assessment, post-incident review and oversight for active counter-drone deployments.
6. Treat electronic conspicuity as a tool for accountability, not as a general public tracking system for ordinary operators.
7. Limit access to personal operator attribution data to authorised entities under clear conditions, with audit logging and purpose limitation.
8. Treat drone detection, tracking and attribution data as sensitive operational data requiring retention limits, access controls, audit logs and onward-disclosure rules.
9. Incorporate privacy-by-design into drone security systems, even where privacy and noise are not the central focus of the consultation.
10. Require security assurance for counter-drone and detection vendors used in high-risk environments.

11. Include cyber and supply-chain security requirements for drones and counter-drone systems used in sensitive contexts.
12. Require confidence thresholds, evidence standards and review mechanisms to reduce harm from false positives and misattribution.
13. Use tiered enforcement that distinguishes accidental, negligent, reckless, deliberate and malicious conduct.
14. Make restricted-area rules clear, public, current, map-based and machine-readable.
15. Ensure geofencing supports compliance but does not become an opaque or overbroad private enforcement layer.
16. Develop practical education through retailers, manufacturers, apps, hobby groups, industry associations and public-facing maps.
17. Use the Trusted Information Sharing Network and sector groups to develop critical-infrastructure-specific guidance.
18. Standardise drone security incident reporting for high-risk entities.
19. Publish aggregated transparency reporting on drone security incidents, counter-drone deployments, enforcement outcomes and complaints.
20. Preserve clear authorisation pathways for legitimate commercial, emergency-service, research, media, agricultural and infrastructure-inspection drone operations.

## 21. Closing

Australia should strengthen its ability to detect, identify and respond to negligent, unsafe, criminal and malicious drone activity. The risks identified in the consultation paper are real; drones can bypass traditional physical security, disrupt critical infrastructure, interfere with emergency and aviation operations, conduct surveillance, deliver contraband and create cyber or supply-chain risk.

However, drone security reform should be precise. It should focus on high-risk places and activities, distinguish between different types of capability, protect legitimate users, preserve privacy, govern data sharing carefully and ensure that counter-drone powers are authorised, proportionate and accountable.

A good framework will not simply restrict drones. It will make lawful drone use more trusted, safer and more sustainable while giving authorised agencies and high-risk operators the tools they need to respond to genuine threats.

## REFERENCES


Cyber and Infrastructure Security Centre (2026) Trusted Information Sharing Network. Available at: https://www.cisc.gov.au/how-we-support-industry/partnership-and-collaboration/trusted-information-sharing-network

Department of Home Affairs (2026a) Drones Security Public Consultation Paper. Available at: https://www.homeaffairs.gov.au/forms-subsite/files/drone-security-consultation-paper-2026.pdf

Department of Home Affairs (2026b) Consultation on proposed approaches to Australia's drone security. Available at: https://www.homeaffairs.gov.au/help-and-support/how-to-engage-us/consultations/consultation-on-proposed-approaches-to-australia-drone-security

Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (2024) Aviation White Paper. Available at: https://www.infrastructure.gov.au/infrastructure-transport-vehicles/aviation/aviation-white-paper

Office of the Australian Information Commissioner (2019) Chapter 3: APP 3 Collection of solicited personal information. Available at: https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information

Office of the Australian Information Commissioner (2025) Chapter 11: APP 11 Security of personal information. Available at: https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information