

POLICY WATCHDOG AUSTRALIA

Staying vigilant so you don't have to.

SUBMISSION TO THE DEPARTMENT OF HOME AFFAIRS

Drones Security: Public Consultation Paper

From: Policy Watchdog Australia

Date: 26 May 2026

Website: policywatchdogaustralia.substack.com

Executive Summary

Policy Watchdog Australia supports the Australian Government's objective of strengthening drone security regulation. The existing aviation-safety framework was not designed to address security risks, and the gap is real. The consultation paper correctly identifies the problem.

The concern is not the reform agenda. It is the structural design of the framework within which reforms are to be built.

The paper's deliberate exclusion of privacy from its terms of reference is analytically untenable. Electronic conspicuity — mandatory real-time identification and tracking of drone operators — is, by definition, a mass-surveillance mechanism applied to the general public. Excluding privacy from scope does not reduce this risk; it means the risk will not be properly addressed in the legislation that follows.

The paper's principles-based, deferred-design approach also risks producing skeleton legislation — a term used to describe primary legislation that grants broad executive powers while leaving the substantive policy detail to regulations or subordinate instruments. Skeleton legislation allows Parliament to approve a framework without scrutinising the actual policy. In security-adjacent legislation, this pattern has produced powers that outlast the threats that justified them.

Policy Watchdog Australia's findings are:

#	Finding
1	The security case for reform is sound and overdue. Drones represent a genuine and growing security risk that the existing aviation-safety framework cannot address. Legislative reform is warranted.
2	The exclusion of privacy from the consultation's scope is the most significant analytical failure in the paper's design. Electronic conspicuity is inherently a surveillance mechanism, and its design must address the Privacy Act 1988 (Cth) and data minimisation from the outset.
3	The principles-based approach creates a structural risk of skeleton legislation with inadequate accountability mechanisms — no independent oversight, no merits review, and no mandatory post-implementation review.
4	Counter-drone authorisations without independent oversight and judicial authorisation requirements create misuse risks the paper does not address.
5	The 'mode-agnostic' scope is appropriate in principle but requires explicit definitional boundaries to prevent unintended capture of autonomous vehicles regulated under separate frameworks.
6	The tiered enforcement approach is proportionate and well-designed, and is supported, subject to merits review rights at each tier.

Policy Watchdog Australia makes six recommendations, detailed in Section 3 of this submission.

About Policy Watchdog Australia

Policy Watchdog Australia is independent and non-partisan, dedicated to the rigorous scrutiny of Australian public policy. Guided by principles of transparency, accountability, and national interest, we analyse legislative proposals and government initiatives to ensure they serve the Australian public effectively. Our articles are published at policywatchdogaustralia.substack.com.

1. Introduction and Context

The Australian Government's Drones Security Public Consultation Paper, released April 2026, initiates a reform process the Aviation White Paper committed to: introducing legislation by 2030 to protect Australian communities, infrastructure, and businesses from drone security risks.

The consultation is timely. The existing regulatory framework — administered primarily through aviation safety legislation and the Civil Aviation Safety Authority (CASA) — was not designed to address the security risks the paper identifies: criminal exploitation, critical infrastructure interference, contraband delivery, hostile reconnaissance, and cyber vulnerabilities in networked drone systems. The European examples cited in the paper illustrate the real consequences of regulatory lag. Regulatory frameworks that focused narrowly on aviation safety left governments without the tools to respond when drones were used to disrupt airports and critical infrastructure.

Australia should not replicate that experience. This submission does not dispute the reform agenda. It addresses the structural design of the framework within which reforms are to be developed — specifically, four structural concerns that, if unaddressed at the consultation stage, are likely to be embedded in the legislation that follows.

This submission applies Policy Watchdog Australia's standard analytical protocol to the consultation paper across five questions: what the proposal is actually doing; who bears costs and who benefits; what the likely real-world effects are; what legislative and structural risks the framework creates; and what the accountability and integrity framework requires.

2. Key Issues and Analysis

2.1 The Privacy Carve-Out Is Analytically Untenable

The paper states that 'specific consideration of [privacy and noise impacts] fall outside the scope of the considerations of this consultation.' This is a significant design error that will affect the legislation that follows.

Electronic conspicuity — the mandatory identification and real-time tracking of drones and their operators — is the foundational security tool proposed across multiple reform areas. The paper proposes that authorised entities have access to real-time location, altitude, and operator attribution data. It proposes data-sharing between law enforcement, security agencies, critical infrastructure operators, and event organisers. It proposes that this data support 'compliance action' against operators.

This is a mass-surveillance infrastructure. It applies not to suspected criminals but to all drone operators — the overwhelming majority of whom are legitimate. Its design will determine whether it is proportionate and accountable, or whether it produces a persistent, searchable record of lawful civilian activity that can be accessed, misused, or breached.

The Privacy Act 1988 (Cth), as amended by the Privacy and Other Legislation Amendment Act 2024, applies to personal information collected by Commonwealth agencies. The automated decision-making transparency obligation under that Act commences 11 December 2026. An electronic conspicuity framework that collects operator identity, location, and movement data is squarely within the Privacy Act's scope. Excluding privacy from the consultation does not exclude it from the law.

Policy Watchdog Australia finds that **the privacy carve-out must be removed**. The legislative framework must include data minimisation requirements, defined retention limits, access controls, and a mandatory privacy impact assessment before any electronic conspicuity scheme is operationalised.

2.2 The Principles-Based Approach Risks Skeleton Legislation

The paper is deliberately non-prescriptive. Its six reform areas are framed as outcomes ('enhance Australia's capacity'; 'deter misuse and enable innovation') rather than mechanisms. Substantive policy content — which agencies are authorised, what zones apply, what detection data can be shared, what constitutes 'appropriate safeguards' — is deferred to future legislation and, almost certainly, to subordinate instruments beneath it.

This approach has a legitimate rationale. Drone technology is evolving rapidly. A prescriptive framework enacted today may be partially obsolete by 2030. The paper's technology-neutral design principle is sound.

The risk is that Parliament will be asked to approve an enabling framework with broad powers and vague criteria, while the substantive policy content is left to regulations. Regulations may be disallowable by Parliament, but they routinely pass without scrutiny. The paper does not

propose any independent oversight body for counter-drone authorisations, merits review for zone designations, or mandatory post-implementation review. These omissions at the consultation stage are likely to become omissions in the legislation.

This pattern is recognisable in Australian security legislation. Powers granted for one purpose are routinely applied to others. Sunset clauses are absent. Review mechanisms are internal. Without structural accountability mechanisms built into the enabling framework, the legislation will be difficult to correct once enacted.

Policy Watchdog Australia finds that **the legislative framework must include**: mandatory disallowance procedures for zone designations; an independent oversight mechanism for counter-drone authorisations; and a statutory post-implementation review within three years, conducted by an independent body.

2.3 Counter-Drone Authorisations Require Independent Oversight and Judicial Safeguards

The paper proposes that law enforcement and security agencies receive expanded counter-drone tools and legal powers. It also contemplates that critical infrastructure operators, event organisers, and prison operators may access drone detection technologies. The paper acknowledges that radiofrequency (RF) jamming can affect aviation navigation, mobile networks, and GNSS systems, and that 'only properly authorised and trained operators' should deploy these technologies.

This self-certification model is a structural integrity gap. A framework that authorises counter-drone deployment without a warrant requirement, without merits review of authorisation decisions, and without public reporting on the frequency and location of deployments has no external detection pathway if those powers are misused. 'Properly authorised and trained' is a circular safeguard: the actor whose conduct it is meant to check is also the actor who determines compliance.

Counter-drone technologies are not passive monitoring tools. Radiofrequency jamming and signal interception actively interfere with the electromagnetic spectrum and, in some configurations, with an identified operator's equipment. This is qualitatively different from passive detection. The existing warrant framework for telecommunications interception under the Telecommunications (Interception and Access) Act 1979 (Cth) provides an established constitutional precedent for judicial oversight of active interference with communications systems. A similar threshold is appropriate here.

Policy Watchdog Australia finds that **active counter-drone technologies deployed against an identified operator require judicial authorisation**. Independent oversight of all counter-drone authorisations, with public annual reporting, is the minimum accountability mechanism necessary.

2.4 The Mode-Agnostic Scope Requires Explicit Definitional Boundaries

The paper proposes a framework applying to aerial drones in the first instance, while embedding broader scope for land and maritime drones. The paper's definition of drones

encompasses systems 'autonomously or remotely operated, moving in the air, on the ground, on water, or under water.' The paper acknowledges that future work on land-based drones would need to consider the Automated Vehicle Safety Law currently being developed by the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts.

This boundary acknowledgment is insufficient. Depending on how the definition is translated into legislation, the framework could inadvertently capture autonomous ground vehicles, robotic delivery systems, and other connected devices already subject to separate regulatory frameworks. Definitional scope creep — key terms defined so broadly that the law's reach is wider than its stated policy target — is one of the most common structural failures in enabling legislation.

The mode-agnostic approach is appropriate in principle: the paper's recognition that cross-modal threats (maritime platforms launching aerial drones; land-based drones conducting reconnaissance for airborne systems) require integrated policy settings is correct. The risk lies in implementation. Achieving mode-agnostic security objectives without inadvertently expanding the regulatory perimeter into separately governed autonomous systems requires explicit legislative boundary-setting.

Policy Watchdog Australia finds that **the legislation must include explicit definitional boundaries** distinguishing regulated drones from autonomous vehicles and robotic systems covered by other legislative frameworks, together with a conflict-of-laws provision specifying which framework prevails where overlap exists.

2.5 Tiered Enforcement Is Proportionate

The paper's proposal for tiered enforcement is well-calibrated. Warnings and administrative penalties for lower-level breaches; higher fines, licence suspension, or revocation for reckless conduct; custodial sentences for weaponisation, critical infrastructure attack, or organised crime — this is a proportionate and graduated response that reflects the actual spectrum of risk.

Policy Watchdog Australia supports this approach, subject to two conditions. First, each tier must carry a right of merits review before the Administrative Review Tribunal (ART) or an equivalent body. A tiered enforcement scheme without appeal rights imposes penalties without accountability. Second, the lowest tier — infringement notices for accidental restricted-area breaches — should include a genuine first-offence educational pathway, reflecting the paper's own acknowledgment that many incidents occur through ignorance rather than malicious intent.

2.6 Public Awareness Must Be a Statutory Duty, Not a Discretionary Programme

The paper's commitment to public education is appropriate. Awareness reduces unintentional breaches, supports voluntary compliance, and enables enforcement agencies to focus resources on genuinely harmful conduct.

The concern is implementation. Public awareness campaigns without sustained resourcing become one-off communications exercises. The paper describes public awareness as

something the government 'is exploring.' Exploration is not a commitment. The legislative framework should include a standing obligation on the administering agency to publish, maintain, and update accessible information about zone designations, operating restrictions, and enforcement outcomes — as a statutory duty, not a matter of administrative discretion.

3. Recommendations

Recommendation 1: Remove the privacy carve-out and embed Privacy Act obligations in the electronic conspicuity framework

The Department of Home Affairs should remove the privacy carve-out from the consultation's scope and ensure the legislative framework mandates: data minimisation for all electronic conspicuity data; defined retention limits; access controls restricting use to authorised security and law enforcement purposes; and a published privacy impact assessment conducted before any electronic conspicuity scheme is operationalised.

Rationale: *Electronic conspicuity is a mass-surveillance mechanism applied to legitimate operators. The Privacy Act 1988 (Cth) governs personal information collected by Commonwealth agencies regardless of whether privacy appears in a consultation's terms of reference. Designing the framework without embedded privacy obligations risks producing a surveillance architecture that is disproportionate, difficult to correct after enactment, and vulnerable to data breach or mission creep.*

Recommendation 2: Require zone designations to be established by disallowable legislative instrument, with merits review

The Department of Home Affairs should ensure that all zone designations — no-go zones, restricted zones, and enhanced monitoring zones — are established by disallowable legislative instrument rather than executive determination. Operators materially and adversely affected by a zone designation should have a right of merits review before the Administrative Review Tribunal (ART).

Rationale: *Zone designations directly affect operators' ability to conduct legitimate commercial and recreational activity. Designations made by executive determination, without disallowance rights or merits review, are effectively unreviewable by affected parties. This is inconsistent with the rule-of-law principle that significant decisions affecting individual rights should be independently reviewable on their merits, not merely on procedural grounds.*

Recommendation 3: Establish independent oversight of counter-drone authorisations with mandatory public reporting

The Department of Home Affairs should establish independent oversight of counter-drone authorisations — through the Inspector-General of Intelligence and Security (IGIS), the Independent National Security Legislation Monitor (INSLM), or a new specialist mechanism — with authority to review authorisation decisions, receive complaints, and publish annual public reports on the frequency, location, and outcomes of counter-drone deployments.

Rationale: *Counter-drone technologies actively interfere with the electromagnetic spectrum and can affect aviation navigation, mobile communications, and GNSS systems. Without independent oversight, no external detection pathway exists for misuse. Self-certification of compliance — 'only properly authorised and trained operators' — is a circular safeguard where the actor whose conduct is to be checked also determines compliance. Annual public reporting creates the minimum external accountability necessary.*

Recommendation 4: Require judicial authorisation for active counter-drone deployment against identified operators

The legislative framework should require judicial authorisation — equivalent in threshold and process to a search warrant under the Telecommunications (Interception and Access) Act 1979 (Cth) — before active counter-drone technologies (radiofrequency jamming, signal interception, or physical interdiction) are deployed against an identified operator. For urgent situations where prior authorisation is impractical, a post-hoc judicial review mechanism should apply, with robust record-keeping requirements.

Rationale: *Active interdiction of a drone directly affects the operator's property and, in some configurations, their physical safety. This is qualitatively different from passive detection. The existing framework for telecommunications interception warrant requirements provides constitutional precedent for judicial oversight of active interference with communications systems. Applying a comparable standard to counter-drone interdiction ensures proportionality without preventing urgent operational responses.*

Recommendation 5: Include explicit definitional boundaries distinguishing drones from autonomous vehicles

The legislative framework should include explicit definitional boundaries distinguishing regulated drones from autonomous vehicles, robotic delivery systems, and other connected autonomous systems subject to separate legislative frameworks, including the Automated Vehicle Safety Law under development by the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts. A conflict-of-laws provision should specify which framework applies where overlap exists.

Rationale: *The paper's mode-agnostic definition of drones — systems 'autonomously or remotely operated, moving in the air, on the ground, on water, or under water' — is broad enough to capture autonomous ground vehicles currently being addressed under a separate regulatory process. Definitional ambiguity in enabling legislation is a well-documented source of regulatory duplication, compliance uncertainty, and unintended scope expansion that is difficult to correct after enactment.*

Recommendation 6: Require a statutory post-implementation review within three years, conducted by an independent body

The legislative framework should require a statutory post-implementation review within three years of commencement, conducted by a body independent of the administering agency. The review should have access to enforcement data, counter-drone deployment records, and privacy impact assessments, and should assess effectiveness, proportionality, privacy impacts, and technological developments. The review report should be tabled in Parliament.

Rationale: *Drone technology is evolving rapidly. A framework designed today will face different conditions by 2030 and substantially different conditions by 2033. A mandatory independent review tabled in Parliament — rather than a discretionary internal review — is the minimum accountability mechanism necessary to correct design errors and recalibrate the framework as technology and the threat environment evolve. Internal reviews have no external incentive to identify their own agency's failures.*

4. Conclusion

The Drones Security Public Consultation Paper addresses a genuine and growing security gap. The threat environment it describes is real, and the case for legislative reform is sound. Australia's existing regulatory framework was designed for aviation safety, not security. That gap needs to be closed.

The legislative framework that follows must be designed with the same rigour applied to the threat assessment. A security framework without embedded privacy protections, independent oversight, merits review, and mandatory post-implementation review is not a balanced framework. Security frameworks without accountability mechanisms produce powers that outlast the threats that justified them.

The legislative models exist. Telecommunications interception oversight, IGIS review functions, disallowable instrument requirements, and ART merits review are established Australian mechanisms. What is required is the decision to apply them to drone security with the same discipline the Government is rightly applying to drone threats themselves.

Policy Watchdog Australia welcomes the opportunity to contribute further to the legislative design phase of this reform, and notes that the submissions process is most valuable when submissions are tested against the draft legislation — not only against a consultation paper that defers all substantive design to a future process.

5. Glossary of Terms

Administrative Review Tribunal (ART)	The federal tribunal established in 2024 to conduct independent merits review of Commonwealth government decisions. Replaced the Administrative Appeals Tribunal (AAT). Merits review allows the ART to substitute a correct decision for a wrong one — not merely to assess whether procedures were followed. Most affected individuals can access the ART; most cannot afford judicial review.
CASA (Civil Aviation Safety Authority)	The Commonwealth statutory authority responsible for the safety regulation of civil aviation in Australia, including the current registration and operational rules for commercial aerial drones. The existing regulatory framework is safety-focused; the paper's proposed reforms would create a parallel security-focused framework.
Electronic conspicuity	Technology that broadcasts a drone's identity, location, and altitude to authorised receivers in real time. Designed to improve situational awareness and enable enforcement. Also creates a real-time and potentially persistent surveillance record of all drone operations within detection range — with significant privacy implications for legitimate operators.
IGIS / INSLM	The Inspector-General of Intelligence and Security (IGIS) and the Independent National Security Legislation Monitor (INSLM) are existing independent oversight bodies for Australia's intelligence and national security legislative frameworks. Both provide established models for independent review of security-sensitive activities that are not appropriate for full public transparency.
Merits review	An independent process — typically before a tribunal — in which both the facts and the reasoning behind a government decision are examined, and the decision can be varied or set aside if wrong. Distinct from judicial review, which assesses only whether the decision was lawful. Merits review corrects wrong decisions; judicial review corrects unlawful ones. Most affected people cannot practically access judicial review.
Radiofrequency (RF) jamming	A counter-drone technique that transmits signals on the same frequency a drone uses for remote control, disrupting the operator's ability to direct the device. Effective without physical contact, but can interfere with aviation navigation systems, GNSS receivers, mobile networks, and emergency services communications — creating safety risks the paper acknowledges without resolving.
Skeleton legislation	Primary legislation that creates a broad enabling framework without specifying the substantive policy content — who is covered, what conduct is regulated, what penalties apply, which agencies are authorised. Substantive detail is deferred to

	regulations or subordinate instruments. Parliament approves the framework; the executive determines the substance. Standard regulations are disallowable by Parliament but routinely escape scrutiny.
--	---