Submission to the

Department of Home Affairs

Drones Security Public Consultation

A Case for Accessible
Drone Detection and Sovereign Capability

[redacted]

May 2026

Summary

Drones are a strategic technology for Australia. They are critical to defence and border security, essential to emergency services and disaster response, and increasingly central to productivity growth across agriculture, mining, logistics, and infrastructure. Australia's sovereignty, economic competitiveness, and community safety will increasingly depend on its ability to produce, operate, and govern drone technology. This submission interprets "drone security" in the broadest terms: not only protecting Australia from malicious or negligent drone operations, but ensuring the availability and dependability[1] of Australia's own drone and detection capabilities, and advancing Australia's capacity to leverage drones as platforms for national resilience, economic growth, and the protection of individual rights.

This submission responds to each of the consultation's questions and raises additional considerations for the framework. Three themes run through it:

1. **Make drone detection accessible.** As drones embed into daily life and become privy to our personal and professional environments, individuals and organisations need the ability to detect their presence to exercise legal rights already conferred by Parliament – including the statutory tort for serious privacy invasion introduced in the Privacy Act amendment of 2024. Non-interfering, privacy-preserving detection is safe and technically feasible. The framework should bring detection activity into a governed model that creates a public-private partnership opportunity with strategic impact: building national drone detection infrastructure while upholding individual rights and creating the social confidence necessary for drones to be adopted and used to advance Australia.
2. **Establish governance for autonomous systems.** The framework targets legislation by 2030. By that date, autonomous drone operations will likely be commonplace and AI-driven decision-making aboard drones will be routine. The framework must establish the principle that an autonomous system operating a drone meets the same accountability standards as a human pilot – verifiable identity, demonstrated competence, provenance, and ongoing compliance – before the technology outpaces the governance.
3. **Advance sovereign capability.** Importantly, the consultation paper highlights drones as a threat to be managed. A complete drone security framework should also advance Australia's sovereign capability for drone production, operations, detection, and workforce development. A framework that addresses only protection, without ensuring the availability and dependability of Australia's own capabilities, is likely going to be ineffective and untenable. Allied nations are pairing counter-drone policy with industrial strategy. The framework is an opportunity to build the policy settings that allow individuals and entities to use drones as platforms for growth, productivity, and national resilience.

Finally, this submission proposes that Australia's emergency services represent a force multiplier for sovereign drone capabilities – including operations, coastal and maritime detection, and workforce development – serving multiple framework objectives from a single investment.

[1] *The three objectives of protection, availability, and dependability mirror the established Confidentiality, Integrity, and Availability (CIA) triad that underpins information and cyber security frameworks globally. Applying these principles to drone security as a cyber-kinetic domain ensures policy completeness and coherence with existing national cyber security strategy.*

A note on urgency: The consultation paper states the government is "seeking to act quickly, recognising the need for urgent reform" (page 3), and targets 2030 for legislation. This submission recommends that the framework identify interim measures – administrative actions, regulatory guidance, SOCI directions – that can be implemented before legislation commences. Detection accessibility, critical infrastructure risk management obligations, and emergency services authorisation can all be progressed through existing legislative instruments and administrative powers. Threats and opportunities that exist today and are rapidly evolving – these need an immediate response.

1. Proactive Management of Emerging Drone Threats

> *Are there specific risks unique to maritime or land-based drones that should be addressed differently within a national framework?*

Recommendation: The framework should substantively address maritime autonomous systems alongside aerial drones, and explicitly resolve the jurisdictional dependencies for land-based autonomous systems.

Both maritime and land-based systems present distinct challenges that warrant specific attention.

Maritime: Maritime drones can operate autonomously for extended periods over vast areas without maintaining a radio link, making operator attribution significantly harder than for aerial systems. Australia's 34,000-kilometre coastline, its strategic port infrastructure (including LNG terminals and naval facilities of AUKUS significance), and its exposure to Pacific maritime drug trafficking routes make this a material consideration. The US Coast Guard's deployment of V-BAT drones on patrol cutters contributed to a record US$362 million cocaine seizure in 2025, demonstrating the scale of maritime contraband threat that autonomous platforms can address – and that adversaries can exploit. The Royal Australian Navy established a Maritime Autonomous Systems Unit in April 2026, signalling that the defence establishment recognises this as an operational priority. The civilian framework should do the same – including detection, identification, and enforcement mechanisms appropriate to the maritime domain and its distinct jurisdictional landscape (AMSA, state marine safety, port authorities, Defence maritime law).

Land-based: The consultation paper's scope includes footpath delivery devices and domestic appliances (page 4), but the legal infrastructure these would rely on is still under development. The Federal Automated Vehicle Safety Law – referenced on page 4 as the framework for land-based drones – is not yet enacted. Existing product safety law (Australian Consumer Law) and common law negligence were not designed for autonomous systems that make independent decisions resulting in physical harm. If a semi-autonomous delivery robot injures a pedestrian or an AI-driven domestic device harms a child, the liability chain – manufacturer, software developer, operator, owner – should be clear within Australian law. The framework should clarify which land-based autonomous systems fall within its scope and which are deferred to the Automated Vehicle Safety Law.

> **Additional consideration: Risk-based classification**
>
> The consultation paper's scope encompasses domestic robotic appliances (page 4) through to commercial aerial platforms capable of carrying hazardous payloads. The framework would benefit significantly from a risk-based classification taxonomy (which the consultation paper alludes to but does not expanded upon). For example, the framework could consider a taxonomy that differentiates systems across three dimensions: operational capability (weight, range, payload, endurance), autonomy level (manual through to full AI-driven autonomy), and consequence of compromise or misuse (nuisance through to mass casualty

/ CBRN[2]). Such a taxonomy would enable the proportionate, tiered controls the paper proposes and provide the basis for consistent enforcement across modes.

How can a mode-agnostic, technology-neutral framework ensure legitimate users are not unduly burdened?

Recommendation: Index controls to capability and consequence. Shift the compliance burden upstream to manufacturers through secure-by-design standards, clear liability, and mandatory capability labelling. Use incentives to offset cost and build sovereign industry.

A sub-250g recreational camera drone and a 25kg commercial platform with 40km range and 5kg payload capacity have fundamentally different risk profiles regardless of the operator's stated purpose. Risk-based classification enables proportionate treatment: lighter controls for lower-risk systems, escalating governance for higher-capability platforms.

Critically, the framework should avoid regulating non-interfering detection capability as if it were active interdiction. Non-interfering sensing (receiving signals a drone is already emitting) poses no risk to drone operations and should attract no regulatory burden[3]. Active countermeasures (jamming, signal takeover) carry real collateral risk and warrant strict controls. These are different regulatory domains and should be treated accordingly.

The most effective way to protect users without burdening them is to shift the compliance obligation upstream to manufacturers, drawing on lessons from cyber security:

- **Secure by design and default:** Manufacturers should embed operational constraints (geofencing, Remote ID, fail-safe return-to-home) as factory defaults that require deliberate action to override. Compliant behaviour becomes the default state, reducing the cognitive and operational burden on operators. This mirrors CISA's Secure by Design pledge and the EU Cyber Resilience Act.
- **Mandatory capability labelling:** A standardised, mandatory label on every drone – weight class, range, maximum altitude, payload capacity, autonomy level, conspicuity features, country of manufacture – would reduce the cognitive burden on users and enforcement agencies. At a glance, any operator or officer can determine what the device can do and what rules apply.
- **Clear manufacturer liability:** Autonomous systems operating in physical space should not attract "as is, without warranties" disclaimers. If a manufacturer ships a drone with a defective autonomous navigation system that causes harm, liability should sit with the manufacturer, not the operator who trusted the system to perform as designed.

Additional consideration: Balancing consumer and industry interests

Transferring burden from users to manufacturers without the right support can be counterproductive. The framework should ensure that the burden is not unduly concentrated on any single part of the ecosystem and all participants are adequately incentivised.

- **Incentives to offset compliance cost**: Tax incentives and R&D grants for Australian manufacturers who meet the standards offset this, simultaneously building sovereign capability. Separate R&D grants should support the development of human-safe autonomous protocols. The cost burden should not fall on the end user alone.

[2] Chemical, Biological, Radiological, Nuclear

[3] Doing so unlocks the opportunity to create a national drone detection network through public-private partnership (refer Section 2).

- **International market creation**: If Australia sets rigorous, clear manufacturing standards early, Australian-made drones that meet those standards become export-ready to allied markets adopting similar frameworks – expanding the addressable market and making domestic manufacturing commercially viable. The framework should support creation of such markets through appropriate foreign policy and trade agreements.
- **Grassroots capability**: Australia should foster community-level drone development through maker programs, STEM pathways, and community workshops. Other nations have demonstrated that distributed, community-level drone capability is both achievable and strategically significant. Building a national skills base serves civilian innovation and strategic resilience simultaneously.

2. Counter-Drone Capabilities

> *What safeguards or oversight are important to ensure counter-drone technologies are used safely and proportionately?*

Recommendation: Formally distinguish between three counter-drone capability tiers – non-interfering detection, active detection, and active interdiction – with separate safeguards for each.

Counter-drone capabilities can be fundamentally distinguished into three tiers, each with different risk profiles, requiring proportionate authorisation models and safeguards:

Tier	Capability	Safeguards
Tier – 1 **Non-interfering, privacy-preserving detection**	*Passive technologies that receive drone RF emissions, read broadcast identification beacons, conduct acoustic analysis, or use passive radar.* Passive detection cannot cause a drone to crash, interfere with navigation, or disrupt communications. These can be designed to detect the presence and behaviour of a drone without identifying the operator – separating ambient telemetry from operator identity. It engages no spectrum management, communications, aviation safety, or surveillance device regulation.	Broadly accessible, subject to privacy-preserving data handling requirements (separation of ambient telemetry from operator identity). No special authorisation, licensing, or training should be required. The safeguard is in data access, not in restricting who can listen.
Tier – 2 **Active detection**	*Technologies that emit RF signals for detection purposes, such as active radar or RF interrogation* Active detection does not interfere with drone operation but uses licensed spectrum and requires coordination with the ACMA.	Available to trained operators under ACMA spectrum coordination, with equipment certification to ensure emissions remain within approved parameters. Critical infrastructure operators, emergency services, and event organisers are likely users, alongside law enforcement and defence.

Tier	Capability	Safeguards
Tier – 3 **Active interdiction**	*Counter-drone technologies including jamming, spoofing, signal takeover and kinetic measures.* These directly interfere with drone operation and engage the Radiocommunications Act 1992, the Criminal Code, and potentially the Civil Aviation Act 1988.	These should be restricted to law enforcement, defence, and specifically designated critical infrastructure protection agencies, subject to mandatory training and certification, equipment type-approval, real-time spectrum coordination with the ACMA, mandatory incident reporting for every deployment, and post-incident review to assess collateral impact on nearby communications, navigation, and aviation systems.

Allied jurisdictions have recognised this distinction. The US Safer Skies Act (December 2025) expanded counter-drone authority with explicit differentiation between detection (funded broadly for state and local agencies) and mitigation (restricted to credible threat scenarios with federal oversight). The EU Counter-Drone Action Plan (February 2026) similarly distinguishes detection/tracking/identification from response/mitigation measures.

> *Who should be authorised to deploy drone detection or counter-drone technologies?*

Recommendation: Non-interfering, privacy-preserving detection should be broadly accessible without special authorisation. Active detection and interdiction should be restricted to authorised agencies.

The detailed case for broad detection accessibility – grounded in legal rights, safety, and strategic opportunity – is set out in the response to the following question.

Active detection and interdiction technologies: Law enforcement, defence, and designated critical infrastructure protection agencies, subject to mandatory training, equipment certification, spectrum coordination with the ACMA, and incident reporting.

> **Additional consideration: Emergency services detection and limited operational authority**
>
> Emergency services (surf life saving entities, SES, CFA, Rural Fire Services) routinely operate in environments where unidentified drones pose immediate safety risks to their operations and the public. The framework should consider whether these organisations should be authorised to deploy non-interfering detection and, in defined circumstances, to direct drone operators to cease operations in emergency zones – analogous to their existing authority to direct the public away from hazards. RF-based interdiction should remain a law enforcement function. The broader case for emergency services as sovereign drone capability is set out in the additional recommendation following Section 6.

> *What role should industry and the public play in reporting or helping to identify emerging drone threats?*

Recommendation: Enable organisations and individuals to operate non-interfering detection systems and contribute data to a national aggregation layer, under a governance framework that defines data standards, contribution protocols, quality requirements, and access permissions.

The consultation paper acknowledges (page 12) that sharing drone detection data between government, commercial, and private entities may provide a cost-effective approach given Australia's geographic scale. This submission supports that aspiration and proposes the policy mechanism to realise it: accessible, governed detection.

The case rests on three arguments:

1. **It is required to enable legal rights.** Individuals and organisations already hold rights under the Privacy Act 1988 (as amended 2024), state surveillance device legislation, and property law that they cannot exercise without detection capability. The 2024 amendment introduced a statutory tort for serious invasion of privacy including by drone surveillance – but exercising that right requires the ability to detect the intrusion. Emergency services, critical infrastructure operators, and event organisers have duties of care that extend to threats in their operating airspace. Detection supports the exercise of rights and obligations Parliament has already legislated.
2. **It is safe.** Non-interfering detection, by definition, cannot affect drone operations, communications, or navigation. As long as the framework mandates privacy-preserving data handling – separating ambient telemetry (drone location, heading, altitude, signal type) from sensor metadata (identity and location of the detecting device) – accessible detection presents no risk to operators, the public, or individual privacy.
3. **It creates a strategic public–private partnership opportunity.** A governed, accessible detection model creates national drone detection infrastructure through public–private partnership, simultaneously advancing national security, upholding individual rights, and creating the social confidence necessary for broad drone adoption. The policy approach should be:
    - set broad access policy;
    - mandate detection for critical infrastructure under SOCI;
    - incentivise commercial and industrial adoption through sovereign manufacturing preferences and tax incentives; and
    - let market forces drive individual and community adoption organically.

    These three tracks – mandate, incentivise, permit – progress in parallel, with independent adoption rates. If market forces do not deliver at the required pace, government increases direct investment. This is a no-regrets approach: broad accessibility settings cost nothing to establish, and the strategic upside – a national detection capability built at a fraction of the cost of government-only infrastructure – is substantial.

Detection systems can be designed to be permissioned, with appropriate levels of detail shared with various stakeholders based on their concern and authority. Individuals receive awareness of whether they are at risk from a nearby unauthorised drone operation – and that is their incentive to participate in the detection value chain. Law enforcement is alerted and response triggered. Manufacturers and operators are immediately notified or demerited from their licence. Each participant's incentive to engage is built into the framework.

Reporting pathways must accept structured data from detection systems – not only free-text reports via triple zero. A standardised detection data format (time, location, signal type, duration, identification content) would enable automated triage by receiving agencies. Where the reported drone is lawfully registered and operating within its approved parameters, the system should filter accordingly to manage reporting volume.

Operational records should be tamper-evident, with cryptographic verification of data provenance, distributed corroboration where multiple sensors observe the same event, and permissioned access appropriate to each stakeholder's authority.

3. Identification and Tracking Through Electronic Conspicuity

> *What level of real-time visibility should authorities have?*

Recommendation: When a drone is detected or is broadcasting identification, the data available should include location, altitude, heading, speed, operator identification, and flight purpose.

For private entities, a simple compliance status – as described in Section 2 – is sufficient. For authorities, the full data set enables effective enforcement and incident response.

> *Should drone detection equipment be extended to new user groups?*

Recommendation: Non-interfering, non-RF-emitting detection should require no special authorisation and should be available to any entity or individual, governed through the data-sharing framework described in Section 2 and leveraged for national interest through shared infrastructure and objectives.

> *What drones should be subject to registration or enhanced identification?*

Recommendation: All remotely piloted and autonomous drones above a de minimis weight threshold (250g aligns with international consensus), enforced in phases.

The current exemption of recreational drones from registration makes enforcement of any identification requirements structurally impossible. A digital licence plate has no value without a vehicle registry.

This could be enforced in phases – voluntary adoption initially, mandatory by exception for defaulters or high-risk operations, escalating to blanket enforcement if needed or when it becomes viable.

Deliberate circumvention of identification systems (disabling Remote ID, spoofing broadcast data) should attract asymmetric penalties, treated as an aggravating factor in any enforcement proceeding. Those with intent to evade detection will find ways to disable conspicuity, just as those with criminal intent may alter or hide vehicle licence plates. The penalty must reflect the deliberate nature of the evasion.

> *What other electronic conspicuity technologies could support security outcomes?*

Recommendation: Set performance-based detection standards rather than prescribing specific technologies. Require manufacturers to supply the RF signatures, protocols, and characteristics needed for their drones to be detectable within the national framework.

ADS-B is designed for cooperative air traffic management and assumes the transmitting aircraft wants to be seen. For security applications, the framework must also accommodate non-cooperative detection: RF fingerprinting, protocol analysis, acoustic signature analysis, and passive radar.

Requiring manufacturers to supply detection-relevant data as a condition of market access ensures that new platforms are detectable from the point of sale. This is analogous to

vehicle manufacturers providing emissions data for compliance verification – the manufacturer contributes to the detection ecosystem, not just the operational ecosystem.

Technology-specific mandates risk obsolescence before the framework commences. Australia's defence programs are funding next-generation quantum RF receivers[4] that will fundamentally change the detection landscape. Performance-based standards accommodate both today's implementations and tomorrow's capabilities. The framework should also ensure a pathway for defence-funded detection technologies to transition into the civilian detection layer, thereby promoting supply chain sovereignty.

Additional consideration: The enforcement chain for zone-based controls

The framework proposes zones (no-go, restricted, enhanced monitoring) and penalties, but the chain connecting them requires five sequential steps: (1) define the boundary, (2) detect the intrusion, (3) classify the intruder, (4) attribute it to an operator, (5) enforce a consequence. Zone designations and penalty schedules address steps 1 and 5. Steps 2 through 4 depend on detection infrastructure, classification taxonomy, and identification mandates that the framework needs to build in parallel. Zone data should be published as machine-readable open data (GeoJSON or equivalent) via API, enabling manufacturers, flight planning applications, and detection systems to cross-reference observed activity against published zones in real time.

Additional consideration: Drone-mounted cyber threats

The primary threat from an unauthorised drone is its physical presence – an uncontrolled object in proximity to people, infrastructure, or sensitive environments. However, a drone's cyber capabilities compound this primary threat. An airborne platform provides mobile, position-agile RF access that ground-based attackers cannot replicate. Wardriving [5]has existed for decades, but a drone changes the equation: line-of-sight coverage from altitude, access to otherwise unreachable positions, and the ability to reposition dynamically. Specific threat vectors – including network intrusion from spoofed access points, GNSS disruption of nearby vehicles, and through-wall surveillance using ambient RF – are documented in peer-reviewed research. Major event security risk assessments under the Crowded Places Strategy should be updated to include drone-mounted cyber threats as a specific scenario, alongside the physical threat scenarios already contemplated.

4. Balanced Enforcement

What penalties would most effectively deter unauthorised or unsafe drone operations?

Recommendation: Combine the tiered penalty approach with mandatory Remote ID, broad-based non-interfering detection, and streamlined structured reporting. The most effective deterrent is the probability of identification, not penalty severity alone.

The tiered approach described in the consultation paper is appropriate. However, under current arrangements, the vast majority of drone operators who breach operating rules are never identified. Increasing penalty severity for the tiny fraction who are caught has limited deterrent effect.

Geofencing mandates are a useful compliance aid for legitimate operators but are trivially bypassed on modified or custom-built platforms. Geofencing is a compliance mechanism, not a security control. The framework should not treat them as equivalent.

[4] the QOBRA program under ASCA, delivered by Defence Science and Technology Group in partnership with Infleqtion, announced publicly in May 2026

[5] the act of searching for Wi-Fi wireless networks and Bluetooth devices from a moving vehicle, using a laptop or smartphone equipped with a GPS.

> *What reporting obligations should apply when abnormal drone activity is detected?*

Recommendation: Mandatory structured incident reporting for critical infrastructure operators, correctional facilities, airports, ports, hospitals, and major events. For the broader public, the governed detection framework described in Section 2 provides a reporting mechanism that accepts machine-generated data.

This reduces the burden on both reporters and receiving agencies compared to free-text reporting. Standardised detection data (time, location, signal type, duration, identification content) enables automated triage.

> **Additional consideration: Adversarial testing and continuous improvement**
>
> The framework proposes detection, zones, and enforcement but would benefit from a mechanism for testing whether these controls work in practice. The SOCI Act mandates risk management programs (CIRMPs) for critical infrastructure with four hazard vectors: cyber, personnel, supply chain, and physical. However, a drone-mounted cyber-physical attack bridges the cyber and physical categories in a way neither vector currently addresses. The independent review of the SOCI Act (March 2026) recommended expanding coverage to include drone detection and response, signalling that the gap between drone threats and critical infrastructure risk management is already recognised at the policy level. The framework should align with this direction by introducing drones as a named hazard within the CIRMP's existing cyber and physical security vectors, or by creating a fifth cyber-kinetic hazard vector that addresses threats bridging both categories. It should also require periodic adversarial UAS assessments for critical infrastructure operators, drawing on Australia's existing CORIE framework for intelligence-led adversarial testing in the financial sector and APRA's CPS 234 for information security. These assessments should test the full enforcement chain, including drone-mounted cyber-physical scenarios.

5. Drone Classifications and Operating Restrictions

> *Should specific no-use or enhanced-monitoring zones be designated?*

Recommendation: Yes. Link zone designations to minimum detection requirements for zone operators, or provide a funded detection-as-a-service capability.

The proposed zone categories (no-go, restricted, enhanced monitoring) are appropriate. Their practical value depends on the detection and identification infrastructure that makes them enforceable. A restricted zone without detection capability is an advisory notice.

> *How should zones be communicated?*

Recommendation: Publish zone data as machine-readable open data accessible via API.

This enables drone manufacturers, flight planning applications, and detection systems to consume zone data programmatically. Human-readable communication (signage, app notifications) is necessary but insufficient given the scale of Australia’s airspace and the diversity of its operator community.

> **Additional consideration: Cyber security baselines for commercial drone fleet management**
>
> The consultation paper already contemplates individual drone compromise (Annexure B). Fleet management systems present a distinct, additional risk: a single compromise of a centralised command-and-control platform scales across every drone in the fleet simultaneously. The same vulnerability class that enabled supply chain compromises in enterprise software (SolarWinds, MOVEit, 3CX) applies directly to drone fleet management infrastructure. The framework should consider mandatory cyber security baselines for

commercial fleet management systems, aligned with SOCI's existing risk management requirements where the served industry falls within a critical infrastructure sector.

Additional consideration: Supply chain integrity for detection equipment

The consultation paper correctly identifies supply chain risk from foreign-manufactured drones but the analysis should extend to detection infrastructure. If Australia builds a national detection capability, the detection layer itself becomes a target for compromise. A subverted sensor could report false negatives or exfiltrate intelligence. The framework should establish tiered supply chain integrity requirements: higher assurance for defence and critical infrastructure detection, proportionate requirements for consumer-grade systems.

6. Public and Industry Awareness

> *What information would help the public better understand risks associated with drones across land, air, and maritime domains?*

Recommendation: Communicate both the risks drones present and the rights individuals hold. Most people do not know they now have statutory protections against drone-based privacy invasion.

The public currently lacks basic literacy about drones – most people do not know that drones emit detectable signals, that Remote ID exists, or that the Privacy Act 2024 amendment gives them a cause of action against serious drone-based privacy invasion. Targeted communication that explains what drones broadcast, what rights community members hold under privacy and property law, and how to report drone activity through structured channels would improve reporting quality and public confidence.

Counter-drone awareness is also important: explaining what counter-drone equipment does, why RF jamming is restricted, and the legal consequences of attempting to interfere with a drone. Without this context, there is a risk that frustrated property owners attempt improvised interdiction.

> *What public communication or education would help operators understand their responsibilities?*

Recommendation: Invest in digital tools that make compliance the default, and position awareness as a secondary control that complements technical measures.

The framework should invest in automated zone checking in flight planning applications, manufacturer-integrated geofencing updates, and push notifications for temporary restrictions. These make compliance the path of least resistance.

Additional consideration: Technology should do the heavy lifting

The cyber security industry provides a cautionary precedent. For two decades, human awareness was positioned as a primary defence against phishing and social engineering. The Australian Signals Directorate continues to identify human error as a leading compromise vector despite substantial investment in awareness programs. The industry eventually accepted that security models dependent on humans consistently making correct decisions are structurally fragile. The shift was to technical controls – multi-factor authentication, endpoint detection, zero-trust architecture, secure-by-default design – with awareness as a complement, not a substitute. The framework should ensure that awareness supports compliance by well-meaning operators while primary controls remain technical: detection infrastructure, identification mandates, automated zone enforcement, and structured reporting systems. The cognitive burden on citizens is already substantial; technology should do the heavy lifting.

Additional consideration: Governance of autonomous systems

The consultation paper references AI-enabled autonomy (page 9). For a framework targeting 2030 legislation, this warrants deliberate and detailed consideration. When a drone operates under a machine learning model rather than direct human control, the system's behaviour is probabilistic and there is no pilot exercising real-time judgment. Open-source autonomous navigation stacks combined with commercially available object detection models already allow construction of fully autonomous drones with target-acquisition capability. The framework should establish the principle that an autonomous system operating a drone must meet the same accountability standards as a human pilot: verifiable identity (whose system, what version, when last evaluated); demonstrated competence (tested against expected conditions); provenance (training data, developer, quality controls); and ongoing compliance (operating within approved parameters in real time). How these standards are technically implemented should remain technology-neutral. But the principle – that autonomy does not reduce the obligation of accountability – should be established before the technology outpaces the governance.

Additional Recommendation: Emergency Services as Sovereign Drone Capability Multiplier

The consultation paper asks whether detection equipment should be extended to emergency services. This submission argues that the question understates the opportunity.

Australia's emergency services – surf life saving organisations, CFA, SES, Rural Fire Services – already possess the foundational elements of a distributed drone operations and detection capability: trained RPAS pilots with CASA licences; operational infrastructure at strategic coastal and regional locations; established governance, safety management systems, and incident reporting procedures; and community trust that no government surveillance program or commercial product can replicate.

What these organisations lack is detection tools, legal authority to monitor airspace for non-cooperative drones, and a data-sharing mechanism to contribute observations to the national picture. A modest investment on top of an existing asset base would deliver four policy objectives simultaneously:

1. **Detection capability:** Emergency service bases become nodes in the national detection network.
2. **Sovereign drone operations capacity:** Every RPAS pilot trained, every BVLOS capability achieved, expands Australia's sovereign drone workforce – the pipeline for defence, border protection, disaster response, and critical infrastructure protection.
3. **Community participation and skills development:** RPAS programs attract volunteers, build technical skills transferable to the commercial drone sector, and create career pathways in a growing industry.
4. **Public sentiment and social licence:** The consultation paper identifies social licence as essential (page 4). Drone technology associated with trusted emergency service organisations builds positive public engagement that government or commercial programs cannot.

Life saving organisations operate along Australia's coastline – the environment where the framework's maritime gap is most acute. Extending these programs to include maritime drone capability would address coastal emergency response and maritime domain awareness simultaneously.

Recommendation: The framework should recognise emergency services as a strategic national asset for drone operations and airspace awareness. Investment in their RPAS programs should be funded as national security infrastructure – through the Disaster Ready Fund or equivalent mechanisms – not left to volunteer fundraising and state grant cycles.

The framework should also consider sovereign capability more broadly. The US has issued executive orders on drone dominance and airspace sovereignty. The EU pairs its Counter-Drone Action Plan with an industrial forum and €250M deployment initiative. A drone security framework that addresses the threat without investing in sovereign detection, operations, and manufacturing capability addresses only one dimension of security – protection – while leaving availability and dependability unresolved.

Conclusion

Drones represent both a strategic opportunity and an escalating threat for Australia. As platforms for economic growth, emergency response, defence capability, and community resilience, they are among the most consequential technologies of the coming decade. As vectors for surveillance, disruption, and harm, they present multi-domain challenges spanning national security, critical infrastructure, public safety, individual privacy, and cyber-physical risk. The two are inseparable – Australia cannot capture the opportunity without managing the threat, and a framework that focuses only on the threat will constrain the very innovation it should enable. This consultation is a necessary and welcome step toward a framework that achieves both.

The highest-leverage reform available is making drone detection accessible: formally separating non-interfering, privacy-preserving detection from active interdiction, and enabling broad participation in airspace awareness under appropriate governance. The case is:

- **legal** – individuals hold rights they cannot exercise without detection capability;
- **safe** – non-interfering detection cannot affect drone operations or compromise operator privacy;
- **economic** – accessible detection built through public–private partnership costs a fraction of centralised alternatives;
- **strategic** – emergency services and community adoption create a national asset no single investment could replicate; and
- **no-regrets** – if the market responds, Australia gains a national capability. If it does not, government retains full capacity to invest directly. The policy settings are right in both scenarios.

I welcome the opportunity to provide further detail or participate in working groups established to develop these reforms.

[redacted]

May 2026

Melbourne, Victoria

About the Author

[redacted] is a CASA licensed remote pilot and a volunteer in the emergency services sector. He brings over two decades of experience in cyber security, technology governance, and data-driven transformation. The responses in this submission apply established security principles – protection, availability, and dependability – to drone security as a cyber-kinetic domain, drawing parallels to mature frameworks in aviation security, cyber warfare, and critical infrastructure protection.