

Subject: RE: Input Request: Australian Government Drone Security Public Consultation Paper (April 2026)

Good afternoon,

Thank you for the opportunity to provide input on the Australian Government's Drone Security Public Consultation Paper.

As a commercial drone surveying operator providing essential asset mapping and structural inspection services in the region, these proposed reforms directly affect my operational continuity and my ability to support critical infrastructure maintenance safely.

Below is my detailed feedback regarding the risks, impacts, and opportunities presented by the consultation paper, structured by the relevant policy development areas. I recommend incorporating these points into the whole-of-government submission to ensure that security measures do not inadvertently halt legitimate utility and infrastructure operations.

1. Cyber Security and Supply Chain Risks (Page 9 & Page 22)

- Operational Risk: Outright bans on foreign-manufactured drones or prohibitions on their use would cause severe commercial harm across the sector. In the sub-250g to 7kg market, I heavily rely on globally accessible hardware platforms. Forced replacement would be financially restrictive for an independent operator and would delay my critical network monitoring workflows.
- Proposed Mitigation / Opportunity: Rather than implementing rigid hardware bans, the policy should mandate software-level security controls to mitigate risks of foreign data egress. Implementing frameworks such as mandatory offline "Local Data Modes," local offline syncing, or approved sovereign cloud storage platforms would effectively protect sensitive local geospatial data of utilities without requiring a commercial operator to retire cost-effective, high-performing fleet assets.

2. Enhanced Identification, Registration, and Electronic Conspicuity (Page 11 & Page 14)

- For Drones Under 250g: Imposing physical hardware transponders (such as active RF or ADS-B modules) on sub-250g micro-drones is technologically punitive. As an independent operator utilising these micro-platforms for tight residential mapping or rapid asset inspections in urban Darwin, the added weight severely compromises my battery life, payload margins, and flight stability. The framework should rely on digital-only, app-based check-ins for the sub-250g commercial class.
- For Drones Up to 7kg: While I support operational visibility and accountability to ensure safe airspace integration, any public tracking or identification mechanism must strictly safeguard commercial privacy. The real-time broadcast of exact telemetry data, flight paths, and operator details should be restricted to vetted law

enforcement and regulatory authorities. Broad public availability of this data risks exposing my proprietary surveying locations and data-capture paths to competitors, or alerting malicious actors to high-value commercial hardware assets operating on-site.

3. Drone Classifications and Operating Restrictions / Airspace Management (Page 7, Page 15, & Page 16)

- Operational Risk: The introduction of permanent "no-go" geofenced zones or heavily restricted areas around assets such as ports, transport hubs, and energy networks poses a significant threat to the continuity of critical maintenance. Infrastructure owners and utilities frequently contract a legitimate surveying business like mine to map, monitor, and maintain these exact sites. Blanket geofencing could severely disrupt, delay, or halt these essential operational drone contracts.

- Proposed Mitigation / Opportunity: Establish a "Trusted Commercial Operator" fast-track exemption pathway. If an operator holds a valid Remote Pilot Licence (RePL) and Remote Operator Certificate (ReOC) issued by CASA, and possesses a verified commercial contract, flight authorisation within security-sensitive zones should be automated and standardised. This process should integrate directly into approved flight-planning software to bypass lengthy, opaque, multi-agency manual government approvals.

4. Balanced Enforcement & Protection from Counter-Drone Measures (Page 11, Page 12, & Page 13)

- Operational Risk: An industrial-grade surveying or mapping drone can weigh between 2kg and 25kg, representing a substantial capital investment, and an uncoordinated kinetic or electronic mitigation could cause an uncontrolled descent, posing a genuine safety risk to people and critical utility property on the ground. I have significant concerns about expanding counter-drone (C-UAS) capabilities to non-aviation, private infrastructure, or venue security groups that may lack comprehensive airspace training.

- Proposed Mitigation: Active mitigation measures, specifically radio frequency (RF) jamming or GPS spoofing, must be bound by strict, legally enforceable deconfliction protocols. If my commercial drone is legally broadcasting its registration and approved flight plan via electronic conspicuity frameworks, automated or private counter-drone systems must be legally barred from targeting it. This is critical to prevent catastrophic asset loss, liability disputes, and secondary ground injuries caused by unauthorised signal interference during legitimate inspection flights.

- Technical Vulnerabilities and Malicious Workarounds: It is critical to recognise that standard RF jamming and GPS spoofing are completely ineffective countermeasures against optical fibre (tethered) drone platforms. Because control telemetry, navigation data, and encrypted video feeds travel through a physical, secure fibre-optic line rather than over the air, tethered systems cannot be digitally

hijacked, blocked, or spoofed from the ground. Consequently, actors engaged in malicious activity can easily bypass regional airspace geofencing and active wireless counter-drone defences simply by deploying tethered platforms. Because perpetrators of malicious activity can effortlessly circumvent wireless security controls, the policy framework must focus heavily on the hardware point-of-sale licensing links (detailed in Section 7) to establish absolute accountability, rather than relying solely on signal manipulation defences that tethered drones completely neutralise.

5. Impact on Independent Rural Surveyors and Excluded Category Operators (Page 7 & Page 10)

- **Operational Risk:** The proposed security frameworks risk placing an unsustainable regulatory and financial burden on an independent, rural surveying operation. In regional and remote areas like the Northern Territory, many independent operators function as sole traders utilising the "Excluded Category" framework (commercially operating drones under 250g or under 2kg without a ReOC). An independent micro-business does not have a dedicated compliance team or the administrative capacity to navigate complex, multi-agency security clearance protocols.

- **Proposed Mitigation:** If security compliance, mandatory registration, or geofence unlocking processes are tied exclusively to a complex ReOC structure, an independent rural operator will be systematically locked out of commercial opportunities. The final policy must include a simplified, low-cost compliance pathway specifically tailored for an independent, licensed Remote Pilot Licence (RePL) holder operating without a ReOC. This will ensure that vital regional surveying, agricultural mapping, and local infrastructure support can continue without forcing an independent small business to absorb prohibitive administrative overheads.

6. Capital Loss, Equipment Replacement, and Software Mitigations (Page 9 & Page 22)

- **Operational Risk:** A primary concern across the commercial drone sector is the severe financial impact of potential hardware bans or retrospective equipment mandates, which would disproportionately harm an independent small business while severely disrupting large enterprise operations. ○ *For a Small and Independent Business:* Industrial-grade surveying drones, high-resolution cameras, and specialised payloads (such as LiDAR systems) represent a massive capital investment, with individual fleet assets valued anywhere from \$1,000 to over \$50,000. Forcing an independent operator to purchase and install expensive hardware transponders retroactively, or to completely replace otherwise perfectly functional, high-value equipment due to supply chain restrictions, could cause immediate insolvency.

- *For Large Engineering and Surveying Firms:* Large commercial businesses operating extensive, multi-platform fleets would face compounded logistical and financial strain. Blanket equipment bans or mandatory physical retrofitting would ground entire operational divisions, resulting in extensive project delays,

breach-of-contract liabilities with major clients, and millions of dollars in stranded capital assets.

- Proposed Mitigation: Security concerns regarding foreign manufacturer data pipelines and the risk of third-party data extraction can be thoroughly mitigated through existing software-level configurations rather than the financial destruction of hardware assets. By utilising "Local Data Modes," local offline syncing, offline flight-planning applications, and secure sovereign cloud storage frameworks, an operator can completely isolate sensitive geospatial data and eliminate data egress risks. The Department must support these software-driven mitigations to achieve robust cybersecurity outcomes without destroying the viable capital assets of Australia's commercial drone sector.

7. Mitigating Criminal Misuse Through Linked Licensing Frameworks (Page 11 & Page 14)

- My Commentary on the Identified Risk: Anonymous drone operations near high-risk utility assets represent a severe security gap that current aviation safety rules do not address. Traditional perimeter security is ineffective against untraceable aircraft targeting critical infrastructure.

- My Operational Recommendation: To systematically deter criminal exploitation, the government should expand CASA's existing digital portal (myCASA) to introduce a mandatory link between hardware serial numbers and an individual's Remote Pilot Licence (RePL). CASA already has a registration and pilot accreditation structure in place; leveraging this existing system to ensure any drone over 250g is digitally tethered to a licensed operator's profile at the point of sale or registration will eliminate anonymous operation. This establishes absolute accountability, ensuring that if a drone is intercepted near a sensitive utility asset, law enforcement can cross-reference CASA's database to instantly identify the individual legally responsible, providing a powerful deterrent against targeted criminal misuse.

Conclusion and Recommendations

As an active commercial drone operator based in Darwin, supporting critical mapping, surveying, and infrastructure sectors across the region, I strongly advocate for a submission response that emphasises policy outcomes that favour secure software mitigations, automated compliance pathways, and linked licensing frameworks. This approach effectively protects data security and deters criminal risk without disrupting essential utility asset protection or my own commercial enterprise continuity.

Please let me know if you require any further operational details or clarification on these points for the whole-of-government response.

Kind regards,



Darwin, Northern Territory