THE FUTURE OF POSSIBLE

DJI Submission to the Australian Government Drones Security Public Consultation Paper May 2026

Introduction

DJI welcomes the opportunity to contribute to the Australian Government's public consultation on drone security policy. As the world's leading manufacturer of civilian drones, DJI has a significant commercial and policy interest in ensuring that Australia's regulatory framework is effective, proportionate, and conducive to the continued growth of the drone industry.

DJI products are used extensively across Australia — by farmers conducting crop surveys, emergency services tracking bushfires, infrastructure operators inspecting assets, filmmakers capturing creative content, and thousands of recreational enthusiasts. We are committed to ensuring that our technology is used safely, responsibly, and in compliance with all applicable laws.

We strongly support the Australian Government's objective to protect communities and critical infrastructure from negligent, malicious, or dangerous drone activity. At the same time, we urge the Government to ensure that any new regulatory settings are carefully calibrated to avoid placing disproportionate burdens on the vast majority of law-abiding operators and the businesses that serve them.

DJI brings a unique perspective to this consultation. We have engaged with regulators in the United States, European Union, United Kingdom, Japan, Singapore, and many other jurisdictions. This experience informs our view that effective drone security policy must be built on three pillars:

- **Industry partnership**: Manufacturers are well placed to implement security-by-design features at scale.
- **Proportionate regulation**: Rules should be risk-based and avoid over-reach that stifles legitimate use and innovation.
- **Education and compliance culture**: Most incidents result from ignorance, not malice — education is often more effective than enforcement.

DJI has proactively developed a suite of safety and security features, including:

- **Geo-awareness data and alerts:** DJI apps display restricted areas and provide in-app warnings to make operators aware of restrictions and help them comply.
- **Remote ID compliance**: DJI products sold in markets with Remote ID mandates (including the United States, Japan, and EU) are already compliant, and we are ready to support equivalent Australian requirements.
- **Altitude limits**: Default settings and configurable limits to help operators operate within CASA rules.
- **Return-to-home and failsafe systems**: Automated safety responses when signal is lost or battery is critical.

We encourage the Government to engage with manufacturers like DJI as active partners in policy design and implementation, rather than treating products solely as a source of risk.

The consultation paper notes that some countries' laws may compel technology companies to provide data or system access to state actors. DJI takes data security and privacy extremely seriously. We have taken significant steps to address these concerns, including commissioning independent audits by firms such as FTI Consulting and Kivu Consulting as well as a recent audit by OnDefend completed this month. These audits found no evidence of data being transmitted to unauthorised parties. DJI has also established a "Local Data Mode" that prevents any internet connectivity during flight and restricts data shared with DJI using an opt-in model for data sharing versus opt-out.

We urge the Government to base any supply chain security requirements on transparent, evidence-based risk assessments rather than blanket country-of-origin restrictions, which are both commercially distorting, harmful to operators, and technically insufficient to address genuine cyber risks.

Responses to Consultation Questions

Proactive Management of Emerging Drone Threats

> ***Are there specific risks you believe are unique to maritime or land-based drones that should be addressed differently within a national framework?***
>
> DJI does not currently manufacture maritime or land-based products and so has no standing on this question.

> ***How can a mode-agnostic, technology-neutral framework ensure legitimate commercial and recreational users are not unduly burdened while still mitigating security risks?***
>
> DJI recommends the framework specify what security outcomes are required (e.g., real-time identification, geofencing compliance, incident reporting) and allow industry to demonstrate how their products achieve those outcomes through conformity assessment or certification schemes. This approach accommodates rapid innovation — including technologies not yet developed — while maintaining clear accountability. Specific exemptions or simplified pathways for low-risk categories, such as sub-250g drones used recreationally in non-sensitive areas, should be retained and clearly defined.

> ***Are there sectors that may face disproportionate impact from an all-modes approach, and how should government address these impacts?***
>
> Rural operations, for example, agricultural operators — particularly those using large autonomous spraying drones in remote areas — could face disproportionate impact if remote identification or real-time tracking requirements assume reliable mobile or satellite connectivity. The Government should consult sector-specific industry bodies and provide for regulatory accommodation in areas without reliable connectivity. Small business operators in the creative and inspection sectors, who rely on drone services as a core income stream,

should be consulted specifically on the compliance cost impacts of any registration, identification, or licensing changes. Many drone service providers are single employee or 2-3 person entities, without an ability to absorb high compliance costs.

Strengthened Counter-Drone Capabilities

What safeguards or oversight do you think are important to ensure counter-drone technologies are used safely, proportionately, and appropriately?

Counter-drone (C-UAS) technologies — particularly radio-frequency jamming and GPS spoofing — carry significant collateral risks to legitimate airspace users, communications infrastructure, and navigation systems. DJI recommends the following safeguards: (1) A mandatory authorisation and licensing regime for all active C-UAS technologies, administered by CASA; (2) Mandatory training and competency standards for all C-UAS operators; (3) Clear use-of-force protocols specifying when interdiction (as opposed to detection only) is authorised, and by whom; (4) Post-incident reporting requirements and independent oversight; (5) Liability frameworks that allocate responsibility for collateral damage from C-UAS deployment; and (6) Prohibition on the use of C-UAS technologies by private parties without explicit authorisation. Passive detection systems — radar, acoustic sensors, optical cameras — should face a lower bar for authorisation, as they pose no electromagnetic interference risk.

Who should be authorised (with appropriate training and approvals) to deploy drone detection or counter-drone technologies?

DJI recommends a tiered authorisation model. Tier 1 — Passive detection only (radar, RF detection, optical systems): should be available to a broad range of users including critical infrastructure operators, correctional facilities, event organisers, and port authorities, subject to registration and basic training. Tier 2 — Active non-kinetic C-UAS (RF jamming, GPS spoofing, signal interception): should be restricted to law enforcement, defence, and specifically licensed security providers operating under government contract, with mandatory coordination with CASA. Tier 3 — Kinetic C-UAS (interceptor drones, directed energy, nets): should be restricted to ADF and AFP/State Police, given the public safety risks involved. This tiered approach balances the legitimate security needs of a wide range of venues and infrastructure operators with the need to prevent indiscriminate or dangerous use of active C-UAS capabilities.

What concerns do you have with expanded or additional counter-drone measures being introduced for authorised groups in Australia?

Our primary concern is the potential for RF-jamming-based C-UAS to interfere with legitimate aviation operations, GNSS navigation, and telecommunications. Airports, hospitals, and densely populated urban areas are particularly sensitive. A secondary concern is proportionality — deploying high-powered C-UAS in response to a recreational drone flying near a restricted area is excessive and risks causing more harm than the drone

itself. We also note that many commercial C-UAS products on the market have not been independently tested and may not perform as advertised, or may cause unintended interference.

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

Without some form of remote identification (RID), it would be difficult for the public to play a meaningful role in reporting incidents. An app-based RID, that showed serial numbers of drones operating nearby could enable something akin to reporting the license plate of a car seen breaking the law. However, reporting mechanisms must include safeguards against vexatious complaints, which risk chilling legitimate drone use. Reports should trigger proportionate responses — investigation, not automatic grounding of the reported drone.

Enhanced Identification and Tracking Through Electronic Conspicuity

What level of real-time visibility (e.g., location, altitude, or operator attribution) should authorities have to detect, track and identify drones operating near sensitive or high-risk environments?

DJI supports a risk-stratified approach to real-time visibility requirements. Near sensitive or high-risk environments (airports, correctional facilities, critical infrastructure, major events), authorised agencies should have access to: real-time drone position and altitude; drone identifier (serial number or registration number); and approximate operator position where technically feasible. In addition, make and model of drone should be displayed to allow a right-sizing of response and an understanding of threat level (for example, is the drone a 250g drone or a 55kg agricultural drone). This data should be made available through standardised interfaces, such as the ASTM F3411 standard currently used in the US and Japan, and should be accessible only by authorised agencies with appropriate data governance protections. This can be done via Broadcast Remote ID and the installation of RID receivers in key high-risk areas. This model is already in use in the US and other jurisdictions and there are multiple technology vendors offering receiver technology.

Should drone detection equipment only be available to law enforcement and security agencies only, or extended to new user groups such as emergency services, prison operators, critical infrastructure operators and event organisers?

Passive detection equipment should be available to a wide range of users, as outlined in our tiered authorisation model above. Correctional facility operators, critical infrastructure managers, and major event organisers have demonstrated legitimate and pressing needs for situational awareness of drone activity in their vicinity. Restricting passive detection to law enforcement would leave significant security gaps and place unreasonable burdens on agencies that cannot be everywhere at once. What matters is data governance: information captured by detection systems should be retained for minimum necessary periods, shared only with authorised agencies, and not used for purposes beyond drone security

management. There may be a reason to expand some information to the general public so that they can report incidents to the authorities. But the general public should only be able to access the serial number and not any registration information attached to that serial number – to avoid any direct confrontations with a drone operator.

Currently only aerial drones used for commercial purposes must be registered. What drones should be subject to registration or other forms of enhanced identification requirements?

DJI recommends extending registration requirements to all aerial drones above 250g regardless of use category, consistent with the approach adopted in the United States, EU, and UK. The 250g threshold has become an internationally recognised standard, reflecting the point at which a drone can cause meaningful harm to a person or property. Below 250g, the risk profile is substantially lower, and registration requirements would be disproportionate. For commercial operators, registration should be integrated with existing CASA licensing frameworks. Costs should be kept low to encourage compliance. Free registration should be considered for recreational users.

What other enhanced identification and electronic conspicuity technologies are available that could support security outcomes?

DJI recommends Broadcast Remote ID (the current international standard, based on Bluetooth or Wi-Fi signal). Any manufacturer currently selling in the US, EU or Japan should be able to quickly implement Broadcast Remote ID via a firmware update. We caution against mandating ADS-B for most drones, as it is designed for crewed aviation separation and introduces significant cost and complexity without commensurate benefit for drone security. DJI have been informed by one national aviation authority that a rollout of ADS-B broadcasting technology across a manufacturer like DJI could saturate the signal.

Balanced Enforcement That Deters Misuse and Enables Innovation

What penalties or consequences would most effectively deter unauthorised or unsafe drone operations near sensitive locations while remaining fair and proportionate?

DJI supports a tiered enforcement approach. For minor, first-time, or unintentional breaches (e.g., inadvertent entry into a restricted zone by an operator who was unaware of the restriction), warnings and infringement notices with modest financial penalties are appropriate. Mandatory completion of remedial education should be available as an alternative to financial penalties. For repeated or reckless breaches, higher fines, suspension of operating credentials, and mandatory re-training are appropriate. For deliberate misuse with intent to harm, cause disruption, or engage in criminal activity, criminal penalties including custodial sentences are appropriate and should be commensurate with the harm caused or attempted. DJI specifically supports the criminalisation of drone weaponisation — the adaptation of drones to deliver explosives, hazardous substances, or kinetic projectiles — as a distinct and serious offence.

What reporting obligations should apply when abnormal or unauthorised drone activity is detected (e.g., mandatory incident reporting by infrastructure operators), and how should information be shared with authorities?

DJI supports mandatory incident reporting for operators of critical infrastructure and sensitive facilities when a drone incursion is detected. Reporting should be timely (within 24 hours for non-emergency situations, immediately for situations involving imminent threat), standardised (using a common reporting format to enable aggregation and trend analysis), and directed to a central clearing house — ideally within the Department of Home Affairs — that can analyse patterns and coordinate responses. Reported data should be shared with CASA for regulatory purposes, with relevant law enforcement, and with the drone manufacturer where appropriate, to support geo-awareness database updates. There should also be consideration for how to validate sightings. Remote ID would clearly help in this regard. False sightings of drones (incidents that then turn out to not have been an actual drone) are frequent.

Drone Classifications and Operating Restrictions

Should specific no-use or enhanced-monitoring zones be designated around certain assets (e.g., hospitals, correctional and energy facilities)?

Yes, DJI supports the designation of clearly defined no-fly zones around high-risk assets. We already implement many such zones in our FlySafe geo-awareness system. These zones provide operators clear warnings when approaching restricted areas. We recommend: permanent no-fly zones around correctional facilities, airports (extending existing CASA restrictions and the CASA permissions system to access controlled airspace), nuclear and critical energy infrastructure, and declared defence facilities; enhanced monitoring zones (flight permitted with additional care) around hospitals, major event venues during events, and other sensitive sites as designated by the relevant Minister; and temporary flight restrictions (TFRs) that can be activated rapidly for unplanned events such as emergency operations, VIP movements, or major incidents. Geo-awareness implementations should be coordinated with manufacturers to ensure database updates are reflected in drone software in a timely manner. It should be noted that we recommend geo-awareness (providing clear information and warnings) versus geofencing (a hard lock of an area that prevents the drone from flying into or taking off in a specific location). Our own experience of geofencing shows that it can be difficult to scale effectively as there are numerous exceptions and operators with permission that need to be unlocked and that process can become burdensome. DJI processed over a million unlocks in the last year of its geofencing system. The issue for government would be magnified as it tried to implement a geofencing system across numerous manufacturers and platforms.

What areas should be completely restricted from drone operations (unless approved)?

In addition to those listed above, DJI recommends complete restriction (unless specifically approved) over: active emergency response scenes (fire, police, ambulance operations); proximity to operating aircraft at all airports and aerodromes; above crowds at major public events above a defined threshold (e.g., 1,000 persons); within defined radii of parliamentary precincts and courts; and locations declared as restricted by the relevant Minister for national security purposes, with appropriate judicial or parliamentary oversight of extended declarations.

How should 'no-drone-zones' or enhanced-monitoring zones be communicated, including to ensure proper coordination between enforcement entities and authorised operators?

DJI recommends: (1) Integration into drone manufacturer geo-awareness databases; (2) A publicly accessible, machine-readable API of all designated zones, enabling third-party apps and UTM providers to implement the same restrictions; (3) Physical signage at the boundary of sensitive sites, consistent with road signage standards for recognition; (4) Public awareness campaigns, particularly targeting recreational operators who may not regularly check airspace maps as part of the CASA Know Your Drone campaign. Coordination between enforcement agencies and authorised operators (e.g., photographers accredited at major events) should be managed through a pre-authorisation and identification system, with a single point of contact for event-specific approvals.

Building Public and Industry Awareness

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

Key information gaps that public education should address include: what the actual rules are in plain language, presented in context rather than as lengthy regulatory documents; what areas are no-fly zones and why; what happens if you accidentally fly in a restricted area (and the distinction between an honest mistake and deliberate misuse); how to report a suspected drone misuse incident; and what counter-drone measures may be deployed, what they look and sound like, and what to do if a drone is affected by them. DJI is willing to contribute to public education materials. DJI operate a dedicated safety website and in-app safety guidance that we can adapt to reflect Australian legislative requirements.

What communication channels or resources would make it easiest for operators to understand their responsibilities under a future all-modes framework?

In-app prompts and notifications are the most effective channel for reaching active drone operators at the moment of relevance — immediately before and during flight. DJI's apps already deliver airspace information, geo-awareness alerts, and safety reminders to millions of users. We are open to including Australian regulatory content in these apps. Beyond in-

app channels, we recommend: a single, authoritative government web presence for drone operators (rather than information being spread across CASA, Home Affairs, and state agencies); proactive engagement with drone flying clubs and community organisations; and a dedicated outreach programme for commercial sectors with high drone uptake, such as agriculture, construction, and emergency services.

What public communication or education would help recreational and commercial operators avoid entering restricted airspace and understand their responsibilities?

For recreational operators, the most effective interventions are: point-of-sale information — information about registration, rules, and restricted zones provided at the time of purchase; mandatory pre-flight safety briefings built into drone control apps; and targeted social media campaigns ahead of high-risk periods such as major events, school holidays, and bushfire season. For commercial operators, mandatory training programmes already provide a foundation; these should be updated to include security-specific content alongside safety requirements.

Recommendations Summary

In summary, DJI urges the Australian Government to adopt the following key principles in developing its drone security framework:

- **Partner with industry**: Engage manufacturers as co-designers of security solutions, not just regulated entities. Leverage existing safety features such as geo-awareness and Broadcast Remote ID.
- **Apply proportionate risk-based rules**: Calibrate regulatory requirements to actual risk levels. Avoid blanket restrictions that treat all operators and all drones as equally high-risk.
- **Adopt international standards**: Align with Remote ID and C-UAS standards being developed in the US, EU, and ICAO to support interoperability and reduce compliance fragmentation for globally operating businesses.
- **Protect data and privacy**: Ensure that identification and tracking systems are governed by robust data minimisation and access control requirements.
- **Invest in education**: Prioritise education and awareness campaigns as a cost-effective complement to enforcement, particularly for the recreational sector.
- **Enable innovation**: Maintain flexible, technology-neutral frameworks with regular review cycles that allow new products and services to enter the market without unnecessary regulatory barriers.
- **Apply evidence-based supply chain security**: Assess cyber and supply chain risks on their technical merits, through transparent and independent assessment processes, rather than on the basis of country of origin.

Conclusion

DJI is committed to working constructively with the Australian Government to develop drone security policy that protects communities and critical infrastructure while supporting the continued growth of Australia's drone industry. We have extensive experience engaging with regulators internationally and are ready to provide technical briefings, product

demonstrations, and detailed policy advice to assist in the development of effective and proportionate regulations.

We would welcome the opportunity to meet with the Department of Home Affairs to discuss our submission in further detail.

Respectfully submitted,

Adam Welsh

Head of Global Policy

May 2026