Tech Council of Australia

Proposed Approaches to Australia's Drone Security

Tech Council of Australia Submission

May 2026

Introduction

The Tech Council of Australia (TCA) welcomes the opportunity to respond to the Department of Home Affairs' (the Department) Drone Security Consultation Paper (April 2026). We support government's commitment to introduce new drone security legislation by 2030 and to strengthen Australia's ability to respond to the security risks that may be posed by drones.

TCA is the peak industry body representing Australia's technology sector. Our members include leading global and domestic technology companies who deliver products and services that underpin every sector of the economy, including AI, cybersecurity, the operation or supply of critical infrastructure, counter-drone capabilities and the design and manufacture of uncrewed systems.

TCA convenes the National Security Tech Alliance (NSTA), a forum that brings together leading domestic and multinational technology companies on national security and defence technology issues. This submission was informed through consultation with NSTA members. The views expressed reflect the collective input received during that process, although do not reflect the position of any individual member.

Drones are productivity-enabling technologies embedded across critical sectors of the Australian economy, including in agriculture, mining, construction, logistics, defence and emergency services. They are also an Australian sovereign capability priority. Our overarching position is that any future drone security framework should be proportionate to the risks posed, principles-based, technology-neutral, internationally interoperable and co-designed with industry. Most importantly, the framework must be innovation-friendly to support and encourage the development of drone technology in Australia.

TCA's submission sets out recommendations to inform development of the proposed National Policy Framework and associated measures. As the Department's intended policy design becomes clearer, TCA would welcome the opportunity to engage with the Department further. Throughout this submission, we have sought to engage constructively with government's overarching objectives.

Recommendation 1: Create an innovation-friendly policy framework that avoids regulatory overlap

Subject to final scope and design, TCA **supports** the creation of a principles-based, technology-neutral and mode-agnostic National Policy Framework, with a particular focus on protecting critical infrastructure. In principle, the Department's proposed design should enable a regulatory framework that is sufficiently flexible to accommodate rapid developments in uncrewed systems technology.

TCA recommends that any potential reforms be developed in coordination with adjacent government frameworks as a priority, including future Automated Vehicle Safety Laws, Civil Aviation Safety Authority (CASA) regulations, the Security of Critical Infrastructure (SOCI)

framework and the 2023–2030 Australian Cyber Security Strategy. The Department should avoid imposing duplicative or conflicting obligations on industry.

Some of Australia's world-leading drone technology companies currently face existential risks to their commercial viability from regulatory delays, unpredictable approval timelines and increased compliance costs under domestic regulatory regimes. These policy settings must adapt to take advantage of our drone technology opportunity, and any future regulation considered by the Department should avoid imposing further barriers to innovation.

TCA recommends that the proposed National Policy Framework create the conditions for a trusted and accountable drone technology ecosystem that encourages – not inhibits – industry innovation.

Recommendation 2: Explore Remote ID requirements to protect the community and infrastructure

TCA **supports** the Department's intention to enhance Australia's capacity to detect, identify, mitigate and counter malicious or unsafe drone activity. In support of this, TCA recommends the Department consider requirements for drone companies to embed Remote ID technology to allow government, law enforcement and other relevant authorities to track and monitor drone activity.

Remote ID technology transmits flight and identifying information through localised radio signals such as Bluetooth or Wi-Fi, allowing relevant authorities to trace uncrewed systems to pilots or take-off points. Certain Remote ID requirements also currently apply in comparable international jurisdictions (such as the United States and European Union), which could minimise regulatory burden on drone technology companies that already compete in international markets and comply with relevant regulations.

Recommendation 3: Extend counter-drone capabilities to owners and operators of critical infrastructure

While TCA **supports** the Department's intention to strengthen counter-drone capabilities, we recommend that these capabilities extend to owners and operators of critical infrastructure. As the Department's Consultation Paper recognises, drones operating in the air, on land or at sea can be used to interfere with critical infrastructure, posing threats to Australia's national security.

While confirmed malicious incidents on Australian soil are currently rare, the capability, affordability and accessibility of drone technology have increased – and are likely to continue to increase – significantly in the coming years. In consultation with government, owners and operators of critical infrastructure will need to reassess their capacity to respond to drone-related threats, including from unwanted reconnaissance and surveillance, cyber-attacks and other operational disruptions.

Subject to robust safeguards, oversight, approvals and training, designated critical infrastructure operators in the sectors regulated under the SOCI framework – including energy, water, telecommunications, transport and data storage and processing – should be empowered to actively detect and respond to external drone threats. Associated

safeguards could include mandatory certification of counter-drone equipment, operator training and certification, pre-deployment risk assessments, incident reporting and public-private information sharing to support continuous improvement without unnecessarily increasing compliance overhead for industry. We note that reporting thresholds and feedback loops should be actionable and proportionate, ensuring information shared contributes to improved outcomes rather than creating additional compliance burdens without clear operational benefits.

Government's role in establishing a clear authorisation model (e.g. defined roles, approvals and escalation pathways) will be increasingly important where critical infrastructure operators are empowered to utilise counter-drone capabilities. Establishing such a model will ensure accountability and controlled use, and avoid the risks of inconsistent application or uncertainty for operators.

Recommendation 4: Prioritise and plan for the cybersecurity threats posed by drones

TCA **supports** the Department's consideration of cyber risk as part of its drone security reform initiatives. A combination of limited drone detection capability and awareness, a lack of government guidance and increased drone use have led to an environment of drone-related cyber vulnerability in Australia.[1] We recommend the Department treat drones as connected cyber-physical systems from the outset in future regulation – not as standalone aviation assets.

The security risks posed by drones span across identity, communications, telemetry and cloud platforms, not just the devices themselves. The Department's National Policy Framework should embed Secure by Design and Zero Trust across the system architecture, consistent with Australian cybersecurity and critical infrastructure policy. Likewise, the policy framework should take a system-level approach to security, moving beyond fragmented controls to integrated approaches that connect monitoring, reporting and response across the system.

To realise the benefits of a system-level approach, TCA recommends a future policy framework include interoperable, machine-readable standards from drone identification and telemetry. As detection and reporting capabilities expand across government, law enforcement and critical infrastructure operators, common standards are essential to enable real-time coordination and response. Without them, much of the practical value of enhanced visibility and information sharing can be lost.

Conclusion

TCA appreciates the Department's engagement with industry on these reforms and the opportunity to provide input at this stage of the policy development process. The proposals raise important issues for Australia's drone security and for the technology sector that supports it. We welcome the opportunity to discuss this submission further, and to participate in any post-consultation activities.

[1] Simone Chitsinde, Andrew Guimelli and Frank den Hartog, 'Drone-Related Cybersecurity Threats to Australia's Critical Infrastructure'. Innovation Central Canberra (November 2025).