19 December 2025

Dr Jill Slay AM
Independent Reviewer
Critical Infrastructure Security Centre
Department of Home Affairs

Dear Dr Slay,

RE: DroneShield's Submission to the
Independent Review of the *Security of Critical Infrastructure Act 2018*

Thank you for the opportunity to provide a submission to the Independent Review of the *Security of Critical Infrastructure Act 2018*.

This review raises important questions about whether the SOCI Act is meeting its objectives, operating as intended, creating unintended consequences, and addressing emerging threats. DroneShield's submission focuses primarily on the latter. As a world leader in counter-drone technology, DroneShield helps government and law enforcement agencies address the threat of unauthorised drones. Critical infrastructure faces increasing vulnerability to drone-related threats, including espionage, operational disruption and direct payload attacks.

Drones have rapidly shifted from novelty toys to significant security challenges. Across the globe, critical infrastructure, such as airports, energy facilities and data centres have experienced drone incursions. Policy frameworks need to keep up with this evolving threat and ensure that critical infrastructure and the public are adequately protected. In this submission, we argue that the SOCI Act should explicitly recognise and prepare for the threat posed by drones.

Should you have any follow up queries, please do not hesitate to contact [redacted], Government Affairs Manager, at [redacted]

We appreciate your consideration and look forward to contributing further to this important dialogue.

Yours sincerely,

[redacted]

DroneShield's Submission to the Independent Review of the *Security of Critical Infrastructure Act 2018*

The rising drone threat

Across the globe, drones have become a significant and persistent threat to critical infrastructure. An unauthorised drone can cause widespread operational shutdowns, financial losses, and security breaches. This threat spans multiple sectors because drones are highly adaptable and powered by rapidly evolving technologies. Unauthorised drones have been detected at airports and other sensitive sites in Australia, with the risk extending more widely to sectors such as energy, water, healthcare and more.

Under the SOCI Act, critical infrastructure sectors include:

- Communications
- Financial services and markets
- Data storage and processing
- Defence industry
- Energy
- Food and grocery
- Healthcare and medical
- Higher education and research
- Space technology
- Transport
- Water and sewerage

Most of these sectors face a known direct threat vector from drones, and all face an indirect threat, whether through surveillance, disruption, or receipt of harmful payloads.

An unauthorised drone can gather intelligence, interfere with operations, or deliver harmful payloads. Traditional security systems are not designed to account for fast-moving aerial threats. As drone incursions are continuing to occur across the world, nations are scrambling to respond and safeguard against the rising drone threat.

DroneShield recommends that the *Security of Critical Infrastructure Act 2018* explicitly recognise drones as a physical threat vector, and ensure critical infrastructure operators have clear obligations to detect and respond to incursions.

The following sections examine drone vulnerabilities within the transport, energy and health sectors.

Transport Sector

Airports are powerful engines of economic growth and social connectivity. Airports facilitate the movement of people, goods, and services – stimulating trade, tourism, and investment. They also generate billions of dollars in revenue and support thousands of jobs both directly and indirectly. A Deloitte report found that in 2022, airports contributed $105 billion to the national economy or 5 per cent of Australian's GDP[1]. Drone incursions at airports can cause prolonged shutdowns, disrupt thousands of passengers, and cost millions of dollars.

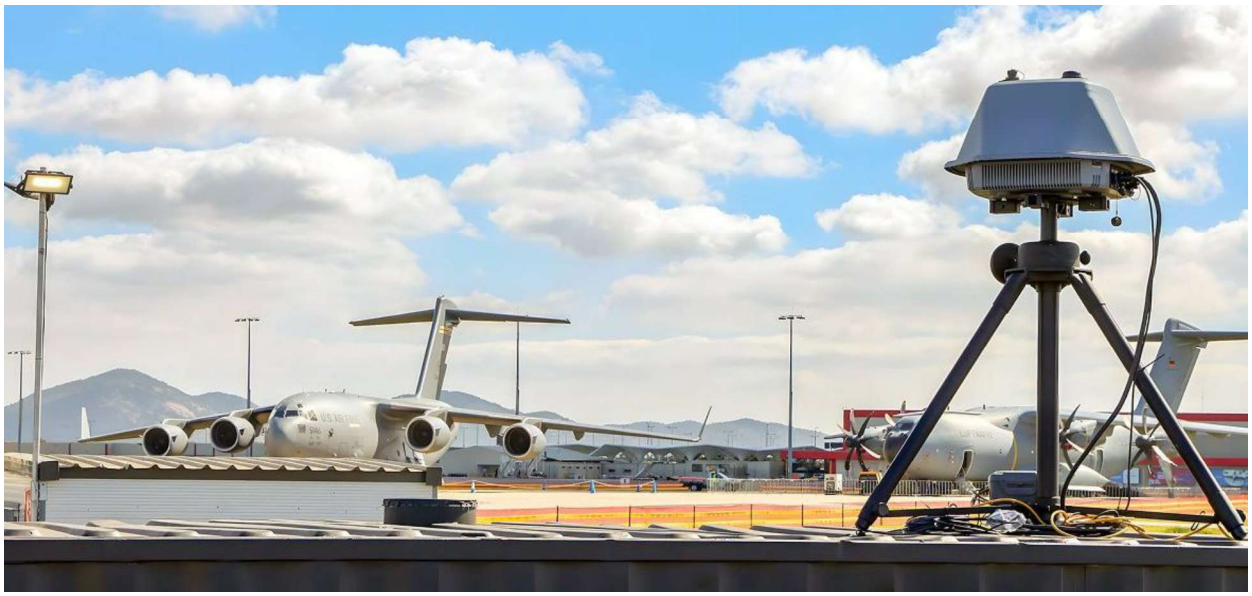

Image: DroneShield's DroneSentry-X Mk2 fixed site drone detection solution at Avalon Airshow, 2025

One of the most well-known airport drone disruptions occurred at Gatwick Airport in December 2018. This event saw two unmanned aerial vehicles close the world's busiest single-runway for 33 hours, across three days in the lead up to Christmas, costing airlines around €50 million in lost revenue and passenger care costs[2]. More recently across Europe, drone incursions have become more familiar. On 22 September 2025, both Copenhagen Airport and Oslo Airport were forced to suspend flights for around 4 hours due to drone sightings[3]. Drone activity around European airports is nothing new, yet the severity of the disruptions has escalated significantly. Commentary by local media outlets found that drone-related disruptions at European airports have increased dramatically, quadrupling between January 2024 and November 2025[4]. European countries are responding, with plans announced for a 'drone wall' by 2030[5], yet the threat remains current and dynamic for airports.

---

[1] Deloitte Access Economics, *Taking Flight: The Economic and Social Importance of Australia's Airports* (Canberra: Australian Airports Association, November 2023), https://airports.asn.au/wp-content/uploads/2023/11/Deloitte-Taking-flight_The-economic-and-social-importance-of-Australias-Airports.pdf.

[2] The Independent, "Gatwick Drone Chaos: Flights Cancelled as Passengers Face Disruption," December 2018, https://www.independent.co.uk/travel/news-and-advice/gatwick-drone-flights-cancelled-passengers-b2466653.html.

[3] BBC News, "Copenhagen and Oslo airports forced to close temporarily due to drone sightings," September 22, 2025, https://www.bbc.com/news/articles/cn4lj1yvgvgo

[4] Euronews. *"Fact-checking Europe's drone problem: Why are airports shuttering over drone sightings."* Euronews, November 20, 2025. https://www.euronews.com/my-europe/2025/11/20/fact-checking-europes-drone-problem-why-are-airports-shuttering-over-drone-sightings.

[5] Annika Burgess with wires, *"Europe unveils 'drone wall' plans to defend against Russia,"* ABC News, 16 October 2025. Available at: https://www.abc.net.au/news/2025-10-17/europe-drone-wall-defence-system-russia-threat-incursions/105893030

Energy Sector

Energy infrastructure underpins every aspect of modern life. Power generation, transmission, and distribution networks fuel industry, households and essential services. In Australia, the energy sector contributes billions of dollars annually to the economy and is central to national security, economic productivity, and social wellbeing[6]. Disruptions to energy supply can impact a range of areas across transport, healthcare, communications and manufacturing, amplifying the impact far beyond the sector itself.

Drones pose a unique and growing risk to energy assets. Unlike traditional threats, drones can bypass perimeter security and reach sensitive areas quickly and cheaply. They can be used to conduct surveillance of substations, pipelines or generation facilities, gathering intelligence on vulnerabilities.

More alarmingly, drones can carry payloads capable of damaging critical equipment or interfere with operations through deliberate collisions. In July 2020, a drone was deliberately modified to damage or disrupt electric equipment at a Pennsylvania power substation. Such modifications of drones require minimal technical skill but have the potential to cause equipment damage, fires, or cascading grid failures[7]. Similar sabotage concerns have been discussed globally, given the ease and impact of such attacks. These risks highlight the need for proactive measures to protect critical energy assets.

Image: DroneShield's DroneSentry-X Mk2 drone detection and defeat solution

[6] Energy Producers Australia, *"Australian Gas Industry's $105 Billion Boost to the Economy,"* Media Release, December 2024, https://energyproducers.au/all_news/media-release-australian-gas-industrys-105-billion-boost-to-the-economy/.

[7] Sean Lyngaas, "Drone at Pennsylvania electric substation was first to 'specifically target energy infrastructure,' according to federal law enforcement bulletin", *CNN*, 4 November 2021. Available at: https://edition.cnn.com/2021/11/04/politics/drone-pennsylvania-electric-substation

Healthcare Sector

Healthcare infrastructure is among the most sensitive and vital components of national resilience. Hospitals, medical supply chains, and pharmaceutical facilities safeguard human life and wellbeing, while also contributing significantly to the economy. In Australia, the healthcare sector employs millions of people and underpins public trust in essential services[8]. Any disruption to healthcare services can have immediate and severe consequences, including delayed treatment, compromised patient safety, and erosion of public confidence.

Drones present a unique and escalating threat to healthcare facilities. Hospital helipads are particularly vulnerable, with a drone incursion during an emergency airlift having the potential to delay critical patient transfers or force helicopters to divert. Drones can also be used to survey sensitive sites, gather intelligence on facility layouts or deliver hazardous payloads to disrupt operations. Even small-scale interference, such as drones flying near hospital emergency entrances, can cause panic, delay ambulances and compromise an emergency response.

As early as 2014, the House of Representatives Standing Committee on Social Policy and Legal Affairs found in their inquiry into drones and the regulation of air safety and privacy that rescue helicopters had been forced to take evasive action to avoid colliding with drones[9]. The rescue helicopter service warned that the consequences of a drone collision could be catastrophic, stating that "even things like birds can damage an aircraft so to run into the UAV or the RPA if you will, you know, that could have been catastrophic."

Image: DroneShield's RfPatrol Mk2 drone detection system used by helicopter operators for enhanced situational awareness

[8] Jobs and Skills Australia, "Health Care and Social Assistance," *Jobs and Skills Australia*, accessed 17 December 2025. Available at: https://www.jobsandskills.gov.au/data/occupation-and-industry-profiles/industries/health-care-and-social-assistance

[9] Commonwealth of Australia, "Report: Eyes in the Sky", Inquiry into drones and the regulation of air safety and privacy, 14 July 2014. Available at: https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Drones/Report

The Australian context

Australia has yet to experience the full scale of disruption from drone incursions witnessed in the United States or Europe. However, as The Asia Group highlights in its report on Counter-UAS and the Protection of Critical Infrastructure, "governments cannot solely rely on the timelines for conventional consultation, legislation, and implementation processes to manage this threat"[10].

Drone attacks on critical infrastructure are a global reality. Australia will inevitably face this threat. Frameworks must empower critical infrastructure operators to deploy appropriate counter-drone technologies so drone incursions can be detected and addressed before they escalate. To safeguard essential services and public safety, critical infrastructure operators should be required to implement protective measures against this evolving risk.

Recommendation

The *Security of Critical Infrastructure Act 2018* does not adequately address the unique risks posed by drones. The legislation should explicitly recognise drones as a physical threat vector and ensure critical infrastructure operators have clear obligations to detect and respond to incursions. These obligations should include mandatory risk assessments, investment in counter-drone technologies capable of detecting non-cooperative drones (those without active signals), and enhanced collaboration between governments, industry and law enforcement.

Without such measures, Australia risks leaving a significant gap in its protective framework, undermining the Act's core objective of safeguarding essential services against evolving and highly accessible threats.

About DroneShield

DroneShield (ASX:DRO) is an Australian headquartered, world-leading innovator in counter-drone solutions. We have one of the largest counter-drone technology focussed research and engineering teams in the world, with around 330 world-class engineers based in Sydney, and Australian based production utilising a substantively Australian supply chain. We both create world leading technologies, as well as act as an integrator of other technologies into complex yet intuitive counter-drone solutions that meet customer requirements.

With deployments by military, intelligence, border security and law enforcement customers in around 50 countries and a strong focus on innovation, DroneShield is at the forefront of drone threat protection. Founded in 2014, DroneShield today has around 46,000 shareholders, most of whom are Australian mum-and-dad retail investors. The 2025 inclusion of DroneShield into the S&P/ASX 200 Index (and being the best performing ASX200 company in 2025 to date) highlights the scale of DroneShield's continued growth and success.

[10] The Asia Group, "Counter-Uncrewed Aerial Systems (C-UAS) and the Protection of Critical Infrastructure. Global Strategies and Best Practices: Implications for Australian Policy", *The Asia Group*, October 2025. Available at: https://theasiagroup.com/wp-content/uploads/2025/10/10.21.25-FINAL-TAG-DS-C-UAS-REPORT-.pdf