

Drones Security

Public Consultation Paper

Department 13 International Pty Ltd
Industry Consultation Response

Department 13 International Pty Ltd		
ABN: 49 639 277 571		
1/28 National Circuit Forrest ACT 2603	+61 1300 376 631	
PO Box 3708 Manuka ACT 2603	info@department13.com	
	Department13.com	

Contents

Executive Summary 3

Proactive management of emerging drone threats 5

Strengthened counter-drone capabilities to protect the community and infrastructure 10

Enhanced identification and tracking through electronic conspicuity 13

Balanced enforcement that deters misuse, and enables innovation 16

Drone classifications and operating restrictions 17

Build public and industry awareness 19

Supporting National Drone Security and Critical Infrastructure Resilience 21

References 23

Release History

Date	Version	Author	Revision Description	Approved By
25/05/2026	1		Industry Consultation	

Executive Summary

Department 13 International Pty Ltd (Department 13) welcomes the opportunity to provide feedback on the Drones Security Public Consultation Paper and supports the development of a nationally coordinated, risk-based and technology-neutral framework for managing evolving drone-related security risks.

The continued growth of drone operations, including beyond visual line of sight (BVLOS) activities, autonomous systems and emerging advanced air mobility platforms, presents both significant economic opportunities and increasingly complex challenges for Australia's aviation, security and critical infrastructure environments. As reflected in the Aviation White Paper: Towards 2050, future aviation policy must balance innovation, operational efficiency and economic growth with strong safety, security and public confidence outcomes.

Department 13 supports the consultation paper's emphasis on protecting critical infrastructure and sensitive sites, improving drone identification and tracking capability, strengthening coordinated national situational awareness, and maintaining proportionate and risk-based regulation. Department 13 also supports the development of stronger operational response capability, enhanced information sharing and reporting arrangements, and future-ready airspace management frameworks capable of adapting to emerging aviation technologies and evolving threat environments.

Our submission also notes the strong alignment between the proposed drone security reforms, the Government's broader Security of Critical Infrastructure (SOCI) reforms, and ongoing work relating to ADS-B, electronic conspicuity and future integrated airspace management systems. Together, these initiatives reflect an increasing recognition that Australia's future resilience will depend not only on regulation, but also on scalable operational capability, persistent situational awareness and coordinated approaches to emerging threats.

In this context, Department 13 believes sovereign operational capabilities such as the Australian Drone Detection Network™ (ADDN) may play an important supporting role in strengthening Australia's broader drone security and critical infrastructure resilience framework. A coordinated drone detection network has the potential to support infrastructure operators, government agencies and authorised stakeholders through improved operational visibility, persistent monitoring, coordinated incident response and enhanced threat awareness across sensitive environments.

Department 13 strongly supports a collaborative approach between government, regulators, infrastructure operators and industry to ensure Australia's future drone security framework remains practical, proportionate, interoperable and capable of adapting to evolving technologies and threat environments.

Department 13 would welcome the opportunity to further contribute to the development of Australia's evolving drone security framework, including through discussion of operational capability, critical infrastructure protection, situational awareness and future integrated drone detection approaches.

This submission has been prepared with regard to the Australian Government's broader aviation, security and critical infrastructure reform agenda, including the Aviation White Paper: Towards 2050, the Drones Security Public Consultation Paper, proposed reforms to the Security of Critical Infrastructure (SOCI) framework, and ongoing consultation regarding the future expansion of ADS-B and electronic conspicuity capability across Australian airspace. Together, these initiatives reflect an increasing emphasis on integrated airspace awareness, operational resilience, coordinated threat detection and the safe integration of emerging aviation technologies.

Proactive management of emerging drone threats

Question: Are there specific risks you believe are unique to maritime or land-based drones that should be addressed differently within a national framework?

Yes. While a common national framework should apply overarching principles across all drone types, maritime and land-based autonomous systems create risks that differ materially from traditional aerial drone operations. Department 13 has identified some of these risks in the sections below although this is not exhaustive. These operational differences may require tailored approaches to monitoring, attribution, detection and response capability within a broader nationally coordinated framework.

Maritime Drones: Maritime drones can threaten subsea cables, offshore pipelines, offshore wind infrastructure, undersea sensors and naval surveillance systems. Unlike aerial drones, maritime systems may physically interact with underwater infrastructure in difficult-to-monitor environments and may operate for extended periods without detection. This is particularly critical given Australia's increasing reliance on subsea communications and energy infrastructure.

Maritime drones can also be used to obstruct shipping channels, interfere with port operations, attach payloads to vessels and conduct covert surveillance of commercial or defence shipping movements. As ports are tightly synchronised operational environments, even minor disruption can create cascading economic and supply chain impacts.

Surface or submersible autonomous systems create unique challenges for border security, drug trafficking, contraband delivery, covert transfer between vessels. Unlike aerial drones, maritime systems can loiter, drift passively or operate semi-submerged, making attribution and interception more difficult.

Maritime drones can operate below radar horizons, semi-submerged, with reduced RF signatures over long endurance periods giving them an advantage within persistent low-signature surveillance. This makes them particularly suited for intelligence collection against ports, naval facilities, offshore assets and of maritime patrol patterns.

Land-based Drones: Land-based drones raise different challenges because they operate within populated urban environments and may interact directly with pedestrians, vehicles and critical public infrastructure. They provide a specific risk for urban infrastructure penetration as they can directly access transport tunnels, rail corridors, public venues, utility easements and underground infrastructure environments. Unlike aerial drones, they can physically enter secured or enclosed spaces while blending into ordinary urban activity.

Ground-based drones can resemble delivery robots, maintenance platforms, logistics systems or mobility devices. This creates specific attribution and enforcement challenges because malicious platforms may appear operationally legitimate within urban environments.

Land systems can directly interact with infrastructure through tampering, cable interference, device placement, payload delivery and physical obstruction. Unlike aerial drones, ground systems may sustain longer physical interaction with infrastructure assets before detection.

Ground systems operating in coordinated groups could potentially disrupt transport hubs, obstruct emergency response vehicles and personnel, overwhelm perimeter security systems and create public panic during major events.

The Aviation White Paper supports a technology-neutral and future-focused regulatory approach, particularly in relation to emerging aviation technologies, integrated airspace management and cross-sector safety governance. Drone and autonomous system technologies continue to evolve rapidly across aerial, maritime and land-based domains, and regulatory approaches that are overly prescriptive or technology-specific risk creating unintended gaps, inconsistencies or loopholes over time. Despite operational differences between these systems, they also present several common challenges from a detection and security perspective, including difficulties relating to attribution, persistent situational awareness, sensor integration, tracking, information sharing and coordinated response across jurisdictions and infrastructure sectors. As autonomous technologies increasingly converge, interoperable detection and monitoring capability across air, land and maritime environments will become increasingly important to supporting critical infrastructure protection, operational resilience and broader national security objectives.

Principles in alignment with the Aviation White Paper application can be applied here by establishing:

- common national security objectives across all drone modes
- mode-specific operational standards and restrictions
- interoperable identification and tracking systems
- harmonised information-sharing arrangements between agencies.

A layered framework will likely avoid fragmented regulation while still recognising the operational differences between aerial, maritime and land-based systems.

Question: How can a mode-agnostic, technology-neutral framework ensure legitimate commercial and recreational users are not unduly burdened while still mitigating security risks?

A mode-agnostic framework should be risk-based rather than technology-prescriptive. The Aviation White Paper repeatedly emphasises proportionate regulation that enables innovation while maintaining safety and public confidence. The framework should therefore distinguish between low-risk recreational use and higher-

risk commercial or sensitive operations by applying obligations according to operational risk, capability and operating environment rather than platform type alone. Factors such as proximity to critical infrastructure, autonomy, payload capability, endurance, beyond visual line of sight operation, swarm capability, and operation within sensitive or densely populated environments should attract higher levels of oversight, identification, monitoring and reporting obligations.

The framework should aim to:

- distinguish between low-risk recreational use and higher-risk commercial or sensitive operations
- apply stronger obligations only where drones operate near critical infrastructure, airports, defence facilities, crowded places or major events or any other facility or facilities covered by the SOCI framework
- provide streamlined approvals and exemptions for compliant operators
- support interoperability with future technologies without requiring constant legislative amendments
- minimise duplication between aviation safety regulation and security regulation.

Recreational users: compliance should remain simple and accessible through clear rules, geofencing, digital notifications and public education.

Commercial operators: particularly those contributing to productivity, logistics, emergency response and regional connectivity, the framework should provide regulatory certainty and nationally consistent rules.

The Aviation White Paper highlights that Australia should embrace technology while maintaining community licence and protecting safety. This balance can best be achieved through scalable obligations linked to operational risk.

Question: Are there sectors that may face disproportionate impact from an all-modes approach, and how should government address these impacts?

Yes. Department 13 believe agriculture, logistics, mining, emergency services, media, infrastructure inspection and regional operators may experience disproportionate compliance costs if regulation is overly broad. All these industries make considerable use of drones in their day-to-day operations.

The Aviation White Paper recognises the importance of regional aviation, general aviation and innovation sectors to Australia's economy and future workforce development. Similar considerations should apply to drone-enabled industries.

Government should consider:

- undertaking sector-specific impact assessments before implementing new requirements
- provide phased implementation timeframes

- prioritise nationally harmonised approvals and standards
- consider grant or rebate programs for compliance technologies such as electronic conspicuity systems
- provide exemptions or streamlined pathways for low-risk operations in remote or regional areas.

Special attention should be given to emergency services and critical response operators to ensure security measures do not unintentionally delay time-critical operations.

The Australian Government's ongoing work to modernise airspace management and support the safe integration of emerging aviation technologies includes consideration of expanded Automatic Dependent Surveillance Broadcast (ADS-B) requirements across Australian airspace. In September 2025, the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA) released a consultation paper examining potential ADS-B mandates for uncrewed aerial vehicles (UAVs) and Advanced Air Mobility (AAM) platforms.

ADS-B is an air traffic surveillance technology that enables aircraft to broadcast identification, position and flight information, improving visibility to air traffic services and other airspace users without relying solely on conventional radar systems. The consultation paper also identified a range of complementary surveillance and electronic conspicuity technologies, including FLARM, Remote ID and ADS-L, which support aircraft visibility, situational awareness and collision avoidance in different operational contexts.

FLARM is commonly used in gliders and recreational aviation for short-range collision warning, Remote ID enables drones to broadcast identification and operational information to support regulatory oversight and airspace awareness, and ADS-L is a lower-power surveillance technology designed for smaller aircraft and uncrewed systems where traditional ADS-B equipment may not be suitable. Together, these technologies reflect the increasing shift toward layered and interoperable surveillance approaches across Australia's evolving aviation ecosystem.

Department 13 considers that broader adoption of ADS-B and electronic conspicuity technologies could significantly improve situational awareness, aircraft separation and the tracking of legitimate or non-malicious drone operations, particularly as BVLOS and autonomous operations continue to expand. However, cooperative surveillance technologies also have important limitations in the context of malicious or non-compliant drone activity because they rely on operators voluntarily broadcasting accurate identification and location data.

Malicious actors may intentionally disable, spoof or avoid electronic conspicuity requirements altogether, including through improvised platforms, modified consumer systems, autonomous flight paths or other non-cooperative approaches specifically designed to avoid conventional airspace awareness frameworks.

The consultation paper also notes that while non-cooperative detection technologies such as radar, optical sensors and LIDAR continue to evolve, they can remain cost, weight or infrastructure prohibitive in some environments.

As a result, Department 13 considers that cooperative technologies such as ADS-B should form part of a broader layered detection ecosystem that also incorporates persistent RF detection and other non-cooperative monitoring capabilities capable of identifying unauthorised, non-compliant or deliberately concealed drone activity around critical infrastructure and sensitive sites.

Strengthened counter-drone capabilities to protect the community and infrastructure

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

Counter-drone powers should operate within a clear legislative framework with strong accountability mechanisms including auditable evidence trails.

Consistent with the Aviation White Paper's emphasis on maintaining aviation safety, community trust and proportionate regulation, safeguards should include:

- strict authorisation requirements for active counter-drone measures
- nationally consistent operational standards and training requirements
- limitations on use to defined high-risk circumstances or protected locations (ie those locations already covered by the SOCI Act or no-fly zones)
- mandatory incident reporting and post-incident review processes
- oversight by an independent regulator
- protections against unnecessary interference with aviation, telecommunications or navigation systems
- clear privacy and data handling requirements.

The framework should also require testing and certification of counter-drone systems to minimise unintended impacts on surrounding infrastructure and aviation operations.

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

Department 13 strongly believe authorisation should be tiered according to risk and capability. Primary authority for active counter-drone measures should remain with Commonwealth and State law enforcement, defence and national security agencies. However, passive detection capabilities should be expanded to cover all Australian critical infrastructure covered under the SOCI Act including but not limited to:

- airports
- critical infrastructure operators
- correctional facilities
- major event operators
- ports

- emergency services.

Department 13 believes that any organisation authorised to use active mitigation technologies should meet nationally consistent requirements for:

- technical competence
- operational governance
- safety management systems
- cyber security protections
- coordination with CASA, Airservices Australia and law enforcement.

This approach aligns with the Aviation White Paper's broader direction to modernise airspace management and integrate new technologies safely into Australia's aviation ecosystem.

This approach would also support the broader objectives of the Security of Critical Infrastructure (SOCi) framework, which increasingly emphasises proactive risk management, operational resilience, and coordinated protection of nationally significant infrastructure from evolving security threats. Capabilities such as the ADDN could assist infrastructure operators and government agencies by improving persistent situational awareness, supporting coordinated incident response, and strengthening resilience across sensitive infrastructure environments.

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

The main risks relate to:

- interference with aviation navigation and communication systems
- disruption to telecommunications and GNSS services
- cyber vulnerabilities in counter-drone systems
- inconsistent operational standards across jurisdictions
- privacy concerns
- mission creep or excessive surveillance powers.

The Aviation White Paper stresses the importance of maintaining community licence and public trust as new technologies are introduced. Expanded counter-drone capabilities must also be accompanied by transparency, public accountability and clear legal limits.

Particular caution is needed around RF jamming technologies in dense urban environments and near airports.

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

Industry and the public should play a structured supporting role. Critical infrastructure operators, airports and major event organisers should have formal reporting obligations supported by standardised reporting pathways.

The public should be encouraged to report suspicious drone activity through simple national reporting mechanisms integrated with existing law enforcement and aviation safety systems.

The Aviation White Paper supports stronger data collection, transparency and reporting across the aviation sector.

Similar principles should apply to drone security by:

- encouraging timely reporting
- standardising incident classification
- supporting coordinated intelligence sharing
- improving situational awareness across agencies.

Public education campaigns will also help distinguish legitimate drone use from genuinely suspicious activity.

Enhanced identification and tracking through electronic conspicuity

Question: 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?

Authorities require access to sufficient real-time operational data to identify risks quickly and respond proportionately.

For operations near sensitive locations, authorised entities should be able to access:

- drone location
- operator/controller location where this is viable
- altitude and direction of travel
- operator registration information
- operational status
- identification serial information
- flight authorisation status where applicable.

Access should be risk-based and limited to **authorised** users with appropriate safeguards.

The Aviation White Paper supports broader use of ADS-B and integrated airspace awareness to support safe aviation operations. Drone identification systems should complement these broader airspace modernisation initiatives rather than duplicate them.

Department 13 believe this would also support the broader intent of the SOCI framework to improve visibility, threat awareness and coordination across critical infrastructure sectors. Shared situational awareness models, including those operated by Department 13, may assist operators and government agencies to identify emerging threats earlier and respond more effectively to incidents affecting sensitive infrastructure environments.

Question: 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?

No. Department 13 strongly believe passive drone detection equipment is critical for national security reasons. Detection capabilities should be expanded beyond law enforcement and security agencies to those operators best able to utilise the information effectively.

Critical infrastructure operators, prisons, airports, ports, emergency services and major event organisers all face legitimate operational risks from drones and should also potentially be permitted to deploy approved **passive** mitigation systems.

However, active mitigation measures such as jamming should remain tightly controlled.

The Aviation White Paper supports collaborative approaches between government, infrastructure operators and aviation stakeholders. A shared situational awareness model would improve resilience and response capability across sectors. Department 13 has included additional information at the conclusion of this submission regarding the Australian Drone Detection Network (ADDN) and its potential role in supporting coordinated drone detection, situational awareness and critical infrastructure resilience capability.

Question: 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?

Registration requirements should be expanded using a risk-based approach.

Registration or enhanced identification should apply to:

- drones above defined weight or capability thresholds
- drones operating beyond visual line of sight
- drones operating near sensitive or restricted areas
- commercial drones
- **autonomous or semi-autonomous systems**
- **drones capable of carrying significant payloads or advanced sensing equipment.**

Low-risk recreational devices operating in ordinary environments should remain subject to simplified obligations.

The Aviation White Paper emphasises proportionate regulation and reducing unnecessary burden while maintaining safety and accountability. This principle should guide any expansion of registration requirements.

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

Potential technologies include:

- ADDN (see section at end)
- remote identification broadcasting
- network-based identification systems
- geofencing integration
- digital flight authorisation systems
- AI-enabled anomaly detection
- integrated traffic management platforms
- encrypted operator authentication systems.

Australia should potentially seek alignment with emerging international standards to support interoperability and reduce compliance complexity for industry.

The Aviation White Paper highlights the importance of future-ready airspace systems and integrated traffic management for new aviation technologies. Drone identification systems should be designed to integrate with these future frameworks.

Balanced enforcement that deters misuse, and enables innovation

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

A tiered enforcement framework would provide the most balanced approach.

Lower-level breaches should attract:

- warnings
- infringement notices
- mandatory education or retraining.

More serious or repeated breaches should attract:

- substantial fines
- suspension or cancellation of licences and registrations
- seizure of equipment.

Deliberate malicious activity involving no-fly zones, critical infrastructure, contraband delivery, espionage or interference with emergency services should attract strong criminal penalties including imprisonment.

The Aviation White Paper consistently supports proportionate, risk-based enforcement combined with stronger accountability and transparency. Drone enforcement settings should follow the same principle.

Question: 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?

Mandatory reporting obligations should apply to airports, ports, critical infrastructure operators, prisons and major event organisers.

Reporting arrangements should:

- use nationally standardised reporting formats
- support near real-time sharing with law enforcement and aviation authorities
- integrate with aviation safety reporting systems where appropriate
- include cyber incident reporting where drone systems are compromised.

The Aviation White Paper places strong emphasis on enhanced reporting, transparency and data-sharing arrangements across the aviation system. Drone security reporting should align with these broader principles. Information sharing frameworks must also include appropriate privacy protections, cybersecurity safeguards and role-based access controls.

Drone classifications and operating restrictions

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

Yes. Department 13 strongly believe certain categories of infrastructure warrant additional protections due to their national security, public safety or operational significance.

Enhanced monitoring or no-use zones should be expanded or implemented around:

- airports and aviation infrastructure
- correctional facilities
- hospitals and emergency response facilities
- defence facilities
- energy infrastructure
- water infrastructure
- telecommunications infrastructure
- major public events
- government facilities and sensitive research sites.

The Aviation White Paper supports stronger approaches to airspace management, community safety and protection of critical infrastructure. Department 13 believe restricted drone operating zones are consistent with these objectives.

These measures would also align closely with broader SOCI reforms focused on improving the resilience of critical infrastructure against evolving and potentially systemic threats. Persistent monitoring capabilities could help operationalise these protections by supporting real-time awareness and coordinated response around nationally significant infrastructure and sensitive locations.

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

Completely restricted areas should include:

- active airport movement areas
- defence installations
- sensitive intelligence and security facilities
- critical national infrastructure assessed as high consequence targets
- emergency incident zones during active operations.

Temporary restrictions should also be available during:

- major events
- natural disasters
- security incidents
- sensitive facilities builds
- high-profile government activities.

Any restricted area framework should remain flexible and capable of rapid adjustment in response to evolving threats.

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

Communication should occur through multiple integrated channels including:

- mandatory geofencing updates
- digital airspace and drone maps
- real-time mobile applications
- NOTAM-style notifications where appropriate
- integrated operator platforms
- public awareness campaigns.
- physical signage where appropriate

The Aviation White Paper places strong emphasis on transparent communication, modernised airspace systems and improved public information. Drone restriction frameworks should align with these broader aviation reforms.

Build public and industry awareness

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

Public education should clearly explain:

- where drones can and cannot operate
- the safety and security consequences of misuse
- penalties for unlawful behaviour
- how drones may affect emergency services and aviation operations
- reporting pathways for suspicious activity
- the difference between legitimate and malicious drone use.

Education should use practical, scenario-based examples tailored to recreational users, commercial operators and industry sectors.

The Aviation White Paper repeatedly highlights the importance of maintaining community confidence and social licence as new aviation technologies are introduced.

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

The most effective communication channels would include:

- a single national digital information portal
- mobile applications with live restriction updates
- mandatory information provided at point of sale
- partnerships with industry associations and hobby groups
- targeted online training modules
- integrated guidance within drone operating software.

Consistency across state governments will be essential to reducing confusion and improving compliance.

Department 13 believe improved collaboration between government, infrastructure operators and operational capability providers will also support the broader objectives of the SOCI framework to strengthen resilience across critical infrastructure sectors. Operational networks can assist by contributing practical threat awareness, operational insights and coordinated communication pathways for sensitive infrastructure environments.

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

Department 13 believe education initiatives should focus on **practical compliance tools** rather than relying solely on written guidance.

This should include:

- mandatory onboarding information during drone registration or purchase
- visual maps of restricted areas
- real-time alerts within drone applications
- public awareness campaigns before major events
- targeted education for high-risk environments such as airports and emergency operations.

The Aviation White Paper emphasises that successful integration of emerging technologies depends on public trust, transparency and effective engagement. Clear and accessible communication will therefore be critical to achieving long-term compliance and maintaining community confidence.

Supporting National Drone Security and Critical Infrastructure Resilience

The policy objectives outlined throughout this consultation paper, including enhanced identification and tracking, protection of sensitive sites, strengthened counter-drone capability, improved reporting, and coordinated national resilience, will require more than regulatory reform alone. Achieving these objectives in practice will depend on the availability of scalable operational capability capable of supporting persistent situational awareness, coordinated response and real-time monitoring across Australia's increasingly complex airspace and critical infrastructure environments.

As drone operations continue to expand, including the anticipated growth in beyond visual line of sight (BVLOS) operations, autonomous systems and advanced air mobility platforms, the challenge of maintaining awareness of drone activity around critical infrastructure and sensitive sites will increase significantly. Traditional site-by-site or standalone monitoring approaches are unlikely to provide the level of coordination, interoperability and operational coverage required to manage evolving drone-related risks at a national scale.

The Aviation White Paper, the proposed Security of Critical Infrastructure (SOCi) reforms, and the Government's broader work on ADS-B, electronic conspicuity and future airspace management all point toward the need for integrated, technology-enabled systems that support improved visibility, operational coordination and resilience across sectors.

In this context, Department 13's Australian Drone Detection Network (ADDN) represents the type of enabling operational capability that could support the successful implementation of many of the consultation paper's proposed reforms. A coordinated sovereign drone detection network has the potential to provide persistent situational awareness around nationally significant infrastructure and sensitive environments, while supporting more effective coordination between infrastructure operators, aviation authorities, law enforcement and national security agencies.

Importantly, a networked approach addresses several structural challenges identified throughout the consultation process. Many critical infrastructure operators do not have the specialist aviation expertise, operational personnel or financial capacity to independently deploy and maintain sophisticated drone monitoring capability. A coordinated shared-service model can therefore provide scalable protection capability while supporting nationally consistent standards, interoperability and information sharing.

A networked capability such as ADDN, which is available on a subscription service, may also support broader national objectives relating to:

- protection of critical infrastructure

- integrated airspace awareness
- future UTM and traffic management systems
- ADS-B enabled detect-and-avoid frameworks
- coordinated incident response
- resilience against evolving and asymmetric threats
- safe integration of emerging aviation technologies.

As Australia's aviation, infrastructure and security ecosystems become increasingly interconnected, persistent drone awareness capability may become an essential component of broader national resilience architecture in much the same way that cyber monitoring, physical security systems and air traffic surveillance are today.

Department 13 would welcome the opportunity to engage further with the Department of Home Affairs on any aspect of this submission or broader considerations relating to drone security, critical infrastructure resilience, operational monitoring capability and emerging airspace management frameworks.

References

References

This response has been prepared with reference to:

Aviation White Paper: Towards 2050 (Australian Government, August 2024)

Drones Security Public Consultation Paper (Department of Home Affairs, 2026)

Proposed Amendments to the Ministerial Directions Powers in Part 3 of the Security of Critical Infrastructure Act 2018 Consultation Paper (Department of Home Affairs, 2026).

Potential Future Expansion of Automatic Dependent Surveillance Broadcast (ADS-B) Mandate in Australia – Consultation Paper (ADS-B Mandate Cross Agency Working Group, September 2025).

Key themes relied upon include:

- protection of critical infrastructure
- proactive national security risk management
- integrated airspace management
- operational resilience
- coordinated threat detection and response
- proportionate and technology-neutral regulation
- enhanced reporting and situational awareness
- public trust and infrastructure resilience
- future-ready security and aviation frameworks
- collaboration between government and industry.

Source documents:

[Aviation White Paper – Towards 2050](#)

[Drone Security Consultation 2026](#)

[Public Consultation Paper - SOCI Act Ministerial Directions Reforms](#)

[Potential future expansion of Automatic Dependent Surveillance Broadcast \(ADS-B\) mandate in Australia—Consultation Paper—September 2025](#)