

Dear Sir/Madam,

I appreciate the opportunity to provide feedback on the *Drone Security Public Consultation Paper* (April 2026).

I am currently employed as the Port Security Officer within a regulated Australian port environment operating under the Maritime Transport and Offshore Facilities Security Act 2003 (MTOFSA). My feedback focuses on the implications of drone security reforms for security regulated ports and maritime supply chain operations.

Alignment with Existing Port Security Frameworks

Australia's ports already operate under legislated security frameworks, including:

- Designated Landside and Waterside Restricted Areas
- Security Regulated Port boundaries
- Maritime Security Levels (MARSEC 1–3)

These controls are designed to manage physical and procedural access to sensitive infrastructure. However:

Drones completely bypass these existing controls.

Traditional measures such as fencing, waterside patrols, and access control points are ineffective against aerial systems, a risk acknowledged in the consultation paper.

At present, drone regulations are largely aviation safety-focused and do not integrate with maritime security frameworks or escalation models. Specifically:

- There is no linkage between drone restrictions and MARSEC levels
- There is no mechanism to dynamically adjust airspace restrictions in response to heightened maritime security threats

Need for Port-Specific Airspace Protection

A critical gap in the current framework is the absence of legally enforceable protected airspace over ports.

I recommend the introduction of:

A legislated Port Protective Airspace Zone, formally recognised within the national airspace framework, and aligned with the boundaries of Security Regulated Ports under the Maritime Transport and Offshore Facilities Security Act 2003, including shipping approach channels and anchorages.

This model should be similar in principle to controlled airspace protections applied to airports, albeit proportionate in scale.

Airports are afforded controlled or restricted airspace due to combined safety and security requirements. Ports present equivalent and, in some cases, more complex risk profiles, including:

- Vessel collision or interference with navigation and pilotage operations
- Intelligence, Surveillance, and Reconnaissance of critical infrastructure
- Delivery of hazardous materials, contraband, or weaponised payloads
- Disruption to berthing, cargo handling, and vessel traffic services

The consultation paper recognises that drones create a three-dimensional threat environment that bypasses traditional security boundaries. This risk is particularly pronounced in port environments with large open waters, extended approach channels, and limited control over offshore launch points.

Without such an airspace overlay, ports remain reliant on ground-based security controls for a threat that operates entirely outside those controls.

Operational Limitations and Enforcement Gaps

A significant challenge for port operators is that:

Port security is regulated but not operationally empowered to respond to drone threats.

Under the current framework:

- Port authorities and security personnel have obligations under MTOFSA but limited direct enforcement powers regarding drones
- The use of counter-drone technologies, particularly those involving radiofrequency (RF) interference (e.g. jamming), is heavily restricted due to safety and telecommunications considerations

This creates a situation where:

- Drone threats can be detected or observed, but
- Immediate mitigation or interdiction is not available at the port level

Without appropriate authorisations or operational frameworks, this represents a critical vulnerability, particularly in time-sensitive or high-risk scenarios.

Security Risk Context for Ports

Ports are explicitly identified in the paper as critical infrastructure and high-risk environments, yet the proposed reforms do not fully address the unique maritime risk profile, including:

- Long-distance vessel approaches and pilotage corridors
- High-value and hazardous cargoes
- Interdependencies with national supply chains
- Increased exposure from both land-based and maritime drone launch points

These characteristics require a dedicated and tailored regulatory overlay, rather than reliance on generalised aviation controls.

Recommendations

To address these gaps, I recommend the following:

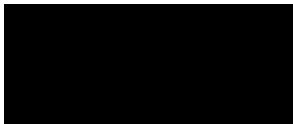
1. **Introduce Port Protective Airspace Zones (PPAZ)**
 - Legally enforceable low-level airspace restrictions over:
 - Security Regulated Ports
 - Waterside Restricted Areas
 - Shipping channels and anchorages
2. **Integrate Drone Controls with MTOFSA and MARSEC Levels**
 - Allow for scalable restrictions based on threat levels (for example, where a change in Maritime Security Level triggers corresponding adjustments to airspace restrictions in coordination with CASA)
3. **Expand Authorised Counter-Drone Capabilities**
 - Consider limited, controlled authorisation for critical infrastructure operators, including ports, to deploy detection and mitigation technologies (Any expansion of counter-drone capabilities should be subject to appropriate training, accreditation, and coordination with Commonwealth and state agencies).
4. **Recognise Shipping Channels as Critical Infrastructure Corridors**
 - Extend protections beyond port boundaries to vessel approach routes

Closing

The consultation paper provides a strong foundation for improving Australia's drone security framework. However, without explicit recognition and integration of port security requirements, significant vulnerabilities will remain within the maritime domain.

Providing ports with appropriate airspace protections and operational authorities will ensure alignment with existing legislative obligations and strengthen the protection of critical national infrastructure.

Thank you for considering this submission.



✉ 298 Marine Terrace, Geraldton, WA, 6530

✉ PO Box 1856, Geraldton, WA, 6531

🌐 www.midwestports.com.au