

25 May 2026
Public

Dronamics Submission to Drone Security Public Consultation Paper 2026

Date: 25 May 2025

Prepared by: Dronamics Group Limited
Contact:

Gavin Gomes, Chief Commercial Officer



I. References

Department of Home Affairs, Drones Security Public Consultation Paper 2026:

<https://www.homeaffairs.gov.au/forms-subsite/files/drone-security-consultation-paper-2026.pdf>

Dronamics (company material shared for consultation) Black Swan platform overview and configurations.

HENSOLDT and Dronamics partnership announcements:

- <https://www.hensoldt.net/news/hensoldt-and-dronamics-announce-a-joint-unmanned-airborne-platform-and-istar-solution>
- <https://www.dronamics.com/post/dronamics-launches-black-swan-defense-platform-and-announces-joint-solution-with-hensoldt%D1%82>

II. Opening statement

Dronamics welcomes the opportunity to respond to the Drones Security Public Consultation Paper 2026. Dronamics designs, builds and operates the Black Swan unmanned aircraft platform to deliver, detect and defend, including long-range, heavy-payload cargo and high-endurance ISTAR/ISR configurations. We support a risk-based, technology-neutral security

DRONAMICS Airlines Australia Delivering Today

Dronamics Airlines Australia Pty Ltd. - Level 20, 123 Eagle Street, Brisbane QLD, 4000
www.dronamics.com

framework that strengthens Australia's ability to detect, identify and respond to negligent or malicious drone activity while enabling legitimate commercial operations and innovation.

Dronamics' approach aligns with the Paper's emphasis on accountability, secure data sharing and proportionate responses. We are NATO interoperable and design for interoperability, including compliance pathways to relevant NATO interoperability architectures and interfaces (e.g., UCS/USAR/ISR interoperability standards) and secure identification and data-link practices. Dronamics is supported by the European Innovation Council (EIC) and has been recognised as a Strategic Technology for Europe.

Supply chain trust and resilience are central to drone security. Dronamics' policy is to avoid sanctioned-state products and materials and to provide supply-chain transparency and compliance attestations to authorised reviewers. Dronamics partners with HENSOLDT for mission systems (ISTAR/AEW sensor suite and mission management) and with Kawasaki Motors for propulsion.

III. Executive summary (key positions)

- Adopt a mode-agnostic, risk-tiered framework that scales obligations with operational risk (e.g., BVLOS, endurance, payload, operating area).
- Prioritise non-kinetic detection and attribution to enable proportionate enforcement and safe responses; restrict active countermeasures to authorised agencies with strict safeguards.
- Implement phased electronic conspicuity (Remote ID / networked identification) and standardise secure data-sharing interfaces and access controls for vetted entities.
- Recognise the role of persistent, distributed surveillance and early warning (airborne ISR/ISTAR/AEW) in protecting critical infrastructure, major events, remote regions and maritime approaches.
- Embed cyber and supply-chain security expectations (secure C2, update integrity, provenance) as core elements of the drone security framework.

IV. Dronamics platform capability relevant to Australia's drone security objectives (public summary)

- Black Swan (Class III) indicative performance: up to ~2,500 km range; payload typically 350–500 kg (mission dependent); endurance up to ~26 hours; runway requirement ~400 m (indicative).
- Multi-role configurations: long-range cargo; long-range, high-endurance ISTAR/ISR; Detect & Defend (counter-UAS support via detection/track and optional effectors subject to local authorisation).

- Sensor/payload capacity: supports multi-domain sensor arrays such as SAR, EO/IR, and ESM/SIGINT (mission dependent) integrated into a fused mission system for Find–Identify–Track–Assess workflows.
- Ground segment: proprietary mobile ground control station concept deployable from a van or container; SATCOM options for wide-area communications; redundancy and cybersecurity measures.
- Industrial capability: sovereign European manufacturing approach with capacity ramp plans; modular design supports local industrial participation and payload integration with domestic industry.

V. Responses mapped to consultation themes

1) Proactive management of emerging drone threats

Recommendation: Establish a national, principles-based framework that enables timely detection, assessment, and response to drone threats across air, land and maritime modes while applying risk-tiered obligations. This should include clear requirements for certified operators (e.g., Safety Management Systems, cyber controls, incident reporting) and structured information sharing through TISN with appropriate safeguards.

Dronamics contribution: Persistent ISR/ISTAR and early warning configurations can support proactive threat monitoring over large geographic areas (including remote regions and maritime approaches), augmenting ground-based sensing and improving attribution time for abnormal or hostile activity.

2) Strengthened counter-drone capabilities to protect community and infrastructure

Recommendation: Strengthen authorised counter-drone capabilities with a “detect–identify–attribute–decide” approach. Non-kinetic detection/track and robust attribution should be prioritised, with active interdiction tools reserved for authorised agencies and operated under strict oversight, safety management, RF/EMI controls, and incident logging.

Dronamics contribution: Black Swan-based airborne surveillance can provide wide-area track correlation and target confirmation to support proportionate decisions by authorised responders, particularly in complex environments (ports, energy assets, major events) where false positives and collateral impacts are a key concern.

3) Enhanced identification and tracking through electronic conspicuity

Recommendation: Implement phased electronic conspicuity requirements (e.g., Remote ID) with privacy-preserving design, and enable secure data sharing between government

and vetted entities. Standardise interfaces to share track-level information (time, location, confidence) and support investigations and enforcement.

Dronamics contribution: Multi-sensor fusion (radar/EO/IR and mission management) can help corroborate identification signals and provide a reliable operational picture when broadcast identification is absent, degraded or spoofed. Dronamics supports secure, role-based access models and audit logging for sensitive feeds.

4) **Balanced enforcement that deters misuse and enables innovation**

Recommendation: Adopt graduated enforcement (education and warnings for low-harm mistakes; stronger penalties for recklessness, repeat offences, contraband delivery, surveillance of sensitive sites, or threats to critical infrastructure). Enable time-limited pilots for accredited operators under safety cases and transparent governance to accelerate safe innovation.

Dronamics contribution: ISR/ISTAR capability can support evidence-quality situational awareness (with appropriate privacy and retention controls) to help enforcement focus on genuinely unsafe or malicious behaviour while minimising burden on compliant users.

5) **Drone classifications and operating restrictions**

Recommendation: Evolve classifications and operating restrictions using risk drivers beyond weight alone, including endurance, payload, BVLOS operation, autonomy, and proximity to sensitive sites. Establish clear “no-go”, “restricted”, and “enhanced monitoring” zones, and ensure these are communicated digitally for geofencing and operator planning.

Dronamics contribution: For certified operations, Australia can consider monitored corridors and structured approvals to enable lawful cargo and special missions while maintaining security oversight. The Black Swan’s runway requirements and endurance profile can be relevant for remote and regional operations.

6) **Build public and industry awareness**

Recommendation: Build public trust through clear guidance, retailer/manufacture partnerships, and transparent explanation of drone security rules, restricted zones and the role of authorised counter-drone measures. For any ISR pilots, implement privacy impact assessments and community engagement to maintain social licence.

Dronamics contribution: Dronamics supports transparency for pilot programs (purpose, governance, safeguards) and will participate in multi-stakeholder exercises and education initiatives as appropriate.

VI. Cross-cutting assurance: NATO interoperability, and trusted supply chains

Drone security policy should explicitly recognise the importance of interoperability and trusted supply chains for government and critical infrastructure use-cases. Dronamics is NATO interoperable and designs for interoperability, including standardised interfaces and secure identification practices (with options for integration subject to Australian requirements). Dronamics' supply-chain policy avoids sanctioned-state products and materials and supports compliance attestations and auditability for authorised reviewers.

VII. Pilot offer (optional)

Dronamics welcomes engagement with the Department and TISN to explore pilots that improve detection, attribution and response coordination in high-risk environments. Potential pilot scopes include maritime approaches and remote critical infrastructure monitoring, with agreed privacy safeguards, data retention controls and performance metrics.

VIII. Conclusion

Dronamics supports reforms that strengthen detection, identification, and proportionate response to drone misuse while enabling lawful innovation. We encourage the Department to prioritise electronic conspicuity, secure information sharing, and governance frameworks that allow non-kinetic detection and attribution to guide safe, accountable counter-drone actions.

Signed,

Gavin Gomes
Chief Commercial Officer, Dronamics Group Limited

