18 May 2026

Attention: Department of Home Affairs, Australian Government

Subject: Drone Consultation

Dear Sir/Madam

SCCN FEEDBACK ON CONSULTATION ON PROPOSED APPROACHES TO AUSTRALIA'S DRONE SECURITY

1. SCCN is an owner and operator of an international subsea fibre optic telecommunications network, with multiple cable landings in Syndey, Australia. SCCL Australia Pty Limited is a licensed Carrier under the Telecommunications legislation. Thank you for the opportunity to comment on the Australian Government's proposed measures to improve drone security outcomes outlined in the Drones Security Public Consultation Paper April 2026.

2. SCCN supports a modernised drone security framework that is risk-based, technology-neutral, and aligned with the protection of critical infrastructure and essential communications networks. From a network security perspective, drones should be treated not only as physical platforms but also as connected digital systems that depend on communications links, navigation services, software, cloud services, and supply chains. Any reform should therefore address both physical misuse and cyber compromise, while preserving legitimate commercial, public sector, and recreational use.

Proactive management of emerging drone threats

3. SCCN agrees that Australia should adopt a mode-agnostic framework, with aerial drones addressed first but with policy settings designed to extend to land and maritime systems where similar security characteristics apply. The key benefit of this approach is consistency across connected platforms that rely on comparable command-and-control links, positioning services, onboard software, firmware updates, and remote data flows. However, implementation should remain risk-tiered to ensure obligations scale according to operating environment, payload, autonomy, connectivity, and proximity to sensitive assets. This will reduce unnecessary burden on low-risk users while allowing stronger controls for systems that could affect telecommunications infrastructure, emergency communications, energy systems, transport networks, or other critical services.

Counter-drone capabilities and safeguards

4. SCCN supports carefully controlled expansion of counter-drone powers for appropriately authorised entities, particularly where critical infrastructure, major events, public safety, or

national security risks are present. From a network security standpoint, any detection or interdiction capability that affects radiofrequency, satellite navigation, mobile services, or nearby communications systems must be subject to strict technical standards, operator accreditation, logging, and post-incident review. Authorisation should be limited to agencies and operators with a clear operational need, demonstrated competence, and defined governance obligations. Passive detection should generally be preferred where feasible, while active measures that may create interference should require higher approval thresholds, tightly defined use cases, and coordination with communications and aviation authorities.

Identification, registration, and electronic conspicuity

5. SCCN supports stronger identification and traceability requirements for drones operating in higher-risk environments, particularly near critical infrastructure, airports, correctional facilities, dense urban areas, and major public events. Real-time visibility should be sufficient to allow authorised entities to identify the drone, assess its location and trajectory, and where lawful and necessary, attribute activity to an operator or operating entity. Registration and conspicuity obligations should be risk-based rather than universal in identical form, with stronger requirements for higher-capability systems, commercial operations, beyond-visual-line-of-sight use, and flights near sensitive sites. Any supporting data-sharing framework should include access controls, retention limits, cybersecurity requirements, and clear rules on when infrastructure operators, regulators, and security agencies may access or share information.

Enforcement, penalties, and reporting

6. SCCN supports a tiered enforcement model that distinguishes between inadvertent non-compliance, reckless conduct, and deliberate malicious activity. This is important to preserve fairness while maintaining strong deterrence for surveillance, interference, contraband delivery, cyber-enabled compromise, or attacks on critical infrastructure. Mandatory incident reporting should apply where operators of critical infrastructure or authorised detection services identify abnormal or unauthorised drone activity that may affect essential services, communications assets, safety systems, or public security. Reporting pathways should be standardised nationally, supported by secure information-sharing arrangements, and designed to produce actionable operational intelligence rather than fragmented notifications across multiple agencies.

Restricted areas, enhanced monitoring zones, and communication to operators

7. SCCN supports clearly defined no-use zones and enhanced-monitoring zones around assets where disruption could have severe public, economic, or national security consequences. This should include selected telecommunications facilities, cable protection zones, energy assets, airports, ports, correctional facilities, defence-related locations, and major event precincts, subject to clear legal definitions and approval pathways for legitimate operations. Restrictions should be communicated through authoritative digital channels, machine-readable data services, and timely updates that can be integrated into operator planning tools and device software where appropriate. Built-in geofencing and digital notices can help reduce accidental incursions, but they should complement, not replace, operator responsibility and formal authorisation processes.

Public and industry awareness

8. SCCN supports targeted education for recreational users, commercial operators, infrastructure owners, manufacturers, and event organisers. Communications should explain not only where drones may or may not operate, but also why network resilience, spectrum integrity, navigation assurance, firmware security, and operator accountability matter for public safety and national security. Industry guidance should encourage secure-by-design procurement, software update hygiene, supply chain due diligence, incident reporting, and coordination with infrastructure security teams. In SCCN's view, the most effective framework will combine proportionate regulation, technical safeguards, trusted information-sharing, and practical education so that Australia strengthens drone security without unnecessarily constraining innovation.

9. Thank you for the opportunity to provide our feedback as a critical infrastructure provider to Australia.

Yours sincerely,

SCCL Australia Pty Limited