AMPOL LIMITED
29-33 BOURKE RD
ALEXANDRIA NSW 2015
ABN 40 004 201 307
ACN 004 201 307

09 June 2026

Department of Home Affairs

Consultation on proposed approaches to Australia's drone security 2026

Part 1 – Introduction:

Ampol Limited **(Ampol)** welcomes the opportunity to make a submission to the Department of Home Affairs **(Department)** regarding the consultation on proposed approaches to Australia's drone security. Drone Security Public Consultation Paper 2026.

As one of Australia's leading fuel suppliers with more than 120 years of operational experience, and as the owner of significant critical infrastructure (CI) (including the Lytton Refinery, terminal and lubricants manufacturing facilities in Queensland, the Kurnell import terminal in Sydney, and the Sydney to Newcastle pipeline network), Ampol would like to provide feedback to the Department on the specific questions posed by the Consultation Paper where Ampol has relevant and substantive comments.

Topic 1: Proactive management of emerging drone threats

The Department is seeking feedback on how a technology-neutral framework applicable to all drone types could be designed. The proposed reforms aim to enable the timely detection, assessment, and mitigation of drone-related threats by authorised counter-drone operators, supported by an adaptable regulatory framework capable of responding to emerging threat vectors as drone technologies evolve.

Ampol considers that any future regulatory framework should include appropriate legislative carve-outs for responsible entities of CI owners and operators that currently utilise drones, uncrewed systems, and other automated equipment as part of their operations. Given the important role these technologies play in the safe and efficient operation, maintenance, monitoring, and security of CI assets, regulatory settings should ensure their continued use is not unintentionally restricted. As the scope of any proposed legislation is not yet known, it is important that exemptions or carve-outs are considered early in the policy development process to avoid unintended operational impacts on CI operators.

Topic 2: Strengthened counter-drone capabilities to protect the community and infrastructure

The Department is seeking feedback on what safeguards are necessary to ensure counter-drone technologies are used safely, proportionately, and appropriately. Ampol highlights the importance of ensuring that any safeguards relating to counter-drone capabilities do not inadvertently impact CI operations, their operational technology systems, or the legitimate use of drones for authorised on-site activities.

CI owners and operators, such as Ampol, should retain the ability to deploy detection and counter-drone capabilities within their own facilities where these measures have been identified as risk-proportionate security control.

Restricting these capabilities solely to government agencies may reduce the ability of CI owners and operators to respond effectively to evolving threats and could limit appropriate security options for CI sites as technology and threat environments continue to develop.

As an alternative approach, instead of limiting detection capabilities, Ampol proposes that consideration could be given to providing exemptions for operators that hold a Major Hazard Facility (MHF) license or that meet another appropriate regulatory threshold. Under this model, the existing licensing and regulatory oversight framework could provide a basis for exempting qualifying CI owners and operators from restrictions on the

use of counter-drone technologies (where those are required to protect CI assets). This approach reduces duplication and recognises the heightened security and safety obligations in place at these assets.

Topic 3: Enhanced identification and tracking through electronic conspicuity

The Department is seeking feedback on the extent to which enhanced identification and electronic conspicuity technologies should be considered to improve operational visibility, accountability, and interoperability with security and safety systems.

Given Australia's geographic scale, consideration should be given to allowing both government and private entities, particularly CI owners and operators, to possess and operate drone detection capabilities. Leveraging existing security and monitoring systems may provide a cost-effective means of identifying and responding to unauthorised drone activity in real time,

Ampol considers that sufficient drone detection capabilities are already available in Australia, and it is essential to retain the ability for CI owners and operators to deploy detection capabilities within their own sites where these have been identified as a risk-proportionate security control.

The decision to implement detection capabilities should adopt a shared responsibility framework, rather than prescribing specific obligations for CI operators to implement detection capabilities. Decisions regarding the deployment of detection technologies should remain with the owner-operator, who is best placed to assess site-specific risks, operational requirements, and security needs. Any regulatory framework should provide flexibility for operators to determine the most appropriate measures for their circumstances and should avoid creating unnecessary barriers to the procurement, deployment, or use of suitable technologies. This would ensure operators can continue to respond effectively to evolving threats while maintaining responsibility for the security of their assets.

Ampol would support requirements for drones to broadcast a digital identity (ID), as this would help distinguish between legitimate hobbyists and potential hostile actors. For site security personnel, remote ID could serve as an initial filtering tool.

While it is acknowledged that hostile actors may seek to circumvent such requirements, a drone operating without a valid or enabled ID module could nevertheless be an early indicator of potential misuse.

By way of example, in April 2026 a drone was observed landing in a vehicle parked outside the Lytton Refinery, Queensland. The activity was identified and managed through Ampol's existing Safety Management Plan and Security Management Plan, with the incident being reported to the relevant authorities.

This incident highlights the value of enabling CI owners and operators to retain and operate appropriate drone detection capabilities. Such capabilities can support the timely identification and assessment of potential threats, facilitate an efficient response, and strengthen coordination with government agencies.

Finally, any implementation should be supported by a reasonable timeframe and developed in consultation with stakeholders to ensure the most effective and practical approach.

Topic 4: Balanced enforcement that deters misuse, and enables innovation

The Department is seeking feedback on what penalties would most effectively deter unauthorised or unsafe drone operations near sensitive locations, and whether reporting obligations should apply when abnormal or unauthorised drone activity is detected (e.g. mandatory incident reporting by infrastructure operators).

Ampol considers that penalties for unauthorised or unsafe drone operations near sensitive or CI should be sufficiently strong to act as a clear deterrent, particularly where such activity presents a safety, security, or operational risk. Penalties should be proportionate to the severity of the breach, with higher consequences for deliberate, repeated, or high-risk interference with CI sites.

Ampol also supports the principle that reporting obligations should apply where abnormal or unauthorised drone activity is detected, particularly in circumstances involving CI. However, such obligations should be designed to be practical and not overly burdensome and should integrate with existing security and incident reporting frameworks to avoid duplication.

Clear guidance should be provided to ensure consistency in reporting thresholds, clear definitions of "unauthorised" or "abnormal" activity, and expectations for response times, to support both regulatory clarity and operational effectiveness.

Topic 5: Drone classifications and operating restrictions

Assets captured under section 12A of the *Security of Critical Infrastructure Act 2018* (Cth) (SOCI Act), including liquid fuel refineries, liquid fuel pipelines, and liquid fuel storage facilities (critical liquid fuel assets), are critical to maintaining the security, reliability, and resilience of Australia's liquid fuel supply chain.

While the proposed framework appropriately focuses on critical liquid fuel assets captured under the SOCI Act, Ampol notes that some infrastructure associated with the liquid fuel supply chain, such as certain terminals and retail sites that do not meet the legislative threshold for CI designation, may also benefit from certain restrictions on unauthorised drone activity from a safety and security perspective. Ampol could work with DFAT and industry stakeholders to explore the development of a framework for identifying critical sites that are not currently captured under the SOCI Act.

Ampol supports the establishment of No-Fly Zones over critical liquid fuel assets and other CI that fall outside the current scope of the SOCI Act, subject to appropriate approvals. Any such restrictions should allow for exemptions where both the asset owner and the Civil Aviation Safety Authority (CASA) have authorised drone operations for legitimate purposes, including surveying, security patrols, asset inspections, and emergency response activities.

CI owners and operators should be recognised as trusted operators, enabling them to conduct flights within their own site perimeters, including designated No Fly Zones, up to a height not exceeding 110% of the tallest on-site structure, without additional restrictions.

As part of one of the priority initiatives identified in the *Aviation White Paper: Towards 2050*, drone policy should establish a dedicated framework for autonomous operations on private land. This framework should reduce the current heavy certification requirements imposed on commercial operators for Beyond Visual Line of Sight (BVLOS) operations and "drone-in-a-box" technologies.

Autonomous and privately owned drones used for 24/7 security patrols or workplace health and safety inspections should be treated as industrial tools rather than conventional aircraft. Where operations are conducted entirely within private boundaries and remain below the height of the tallest on-site structure, these systems should be exempt from current aviation regulatory burden.

Ampol considers that any exemption framework should be tightly controlled and applied only in clearly defined and limited circumstances to ensure ongoing protection of CI while enabling essential operational use cases where required.

Topic 6: Build public and industry awareness

In relation to the Department's request for feedback on what communication channels or resources would help the public better understand risks associated with drones across land, air, and maritime domains, Ampol has no comments to provide at this time.

Conclusion:

Ampol looks forward to continuing to engage constructively with the Department and to providing feedback, particularly on any proposed measures that may potentially create additional burdens for the security management of CI owners and operators.

Should you wish to discuss this submission, please contact [redacted]