jvat
INSPIRING EXCELLENCE

SNC | AUS™

Department of Home Affairs

Drone Security Consultation Paper 2026

Date: 25 May 2026
Document Reference FC3X6URZZQ7T-654712821-3192
Version:1.1

Executive Summary

This joint submission by JVAT and Sierra Nevada Corporation Australia (SNC AUS) responds to the Department of Home Affairs Drone Security Consultation Paper [Reference A] and supports the development of a nationally coordinated, risk-based and technology-neutral framework for uncrewed systems security across aerial, maritime and land domains.

The submission recognises that uncrewed systems are increasingly integrated into legitimate commercial, industrial, emergency service, government and recreational activities, while also presenting emerging safety, security and critical infrastructure risks. Future reforms should therefore remain proportionate, operationally practical and adaptable to evolving technologies including AI-enabled autonomy, autonomous swarming and increasingly software-defined systems.

A central theme of this submission is that Australia's current regulatory and operational arrangements are largely organised by domain-specific legislation and authorities, including aviation safety, maritime safety, radiocommunications, privacy and law enforcement frameworks. As uncrewed systems increasingly operate across and between these domains, there is growing potential for regulatory overlap, operational ambiguity and inconsistent response arrangements. The submission therefore supports nationally coordinated governance arrangements with clearly defined operational authorities, escalation pathways, information-sharing mechanisms and accountability frameworks.

The submission also highlights the importance of distinguishing between passive detection capabilities and active counter-uncrewed system mitigation measures. Detection technologies should be more broadly accessible to approved operators supporting critical infrastructure, emergency response and public safety functions. By contrast, active mitigation capabilities such as RF disruption, protocol takeover or kinetic defeat should remain tightly controlled, proportionate and subject to clear statutory authority, oversight and operational safeguards.

The submission supports a layered and risk-based approach to security, identification and reporting obligations, including enhanced protections for sensitive sites, nationally interoperable reporting mechanisms and improved coordination between government agencies, infrastructure operators and authorised users.

The submission further recommends:

- development of nationally recognised cyber assurance and trusted system frameworks;
- harmonised governance arrangements across Commonwealth, State and Territory agencies;
- improved protection of critical infrastructure and offshore maritime assets;
- scalable registration and identification requirements proportionate to operational risk;
- strengthened public awareness and operator education measures; and
- future regulatory frameworks capable of adapting to emerging autonomous and cross-domain uncrewed system technologies.

Overall, this submission supports a balanced and future-focused regulatory framework that strengthens national resilience, public safety and critical infrastructure protection while enabling responsible innovation, sovereign capability development and legitimate uncrewed system operations across Australia.

Table of Contents

References

A. Commonwealth of Australia, April 2026, *Drone Security Public Consultation Paper*, Department of Home Affairs, Belconnen ACT.

B. FAA, May 2019, *Drone Security Consultation Paper*, US Department of Transportation, Washington DC.

C. FAA, July 2018, *Drone Security Consultation Paper – Attachment 1 – Sponsor Letter*, US Department of Transportation, Washington DC.

D. FAA, July 2018, *Drone Security Consultation Paper – Attachment 2 – UAS Detection Systems FAQs,* US Department of Transportation, Washington DC.

E. FAA, July 2018, *Drone Security Consultation Paper – Attachment 3 – UAS Detection – Technical Considerations*, US Department of Transportation, Washington DC.

F. FAA, DOJ, FCC and DHS, August 2020, *Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems*, Interagency publication, Washington DC.

Acronyms and Abbreviations

Abbreviation	Description
AMSA	Australian Maritime Safety Authority
APS	Australian Protective Services
CASA	Civil Aviation Safety Authority
C-UAS	Counter-Uncrewed Aerial Systems
ELT	Emergency Locator Transmitter
EPIRB	Emergency Position Indicating Radio Beacon
FAA	Federal Aviation Administration
ISR	Intelligence, Surveillance and Reconnaissance
MAAA	Model Aircraft Association of Australia
MOTS	Military Off The Shelf
NOTAM	Notice to Airmen
NTM	Notice to Mariners
PLB	Personal Locator Beacon
RF	Radio Frequency
UAS	Uncrewed Aerial System
USV	Uncrewed Surface Vessels
UUV	Uncrewed Underwater Vehicles

1 Introduction

1.1 Purpose

1.1.1 This document provides a structured industry response to the Department of Home Affairs Drone Security Consultation Paper [Reference A]. JVAT and Sierra Nevada Corporation Australia (SNC AUS) support the development of a nationally coordinated, risk-based and technology-neutral framework for uncrewed systems security that balances:

a. public safety;
b. national security;
c. innovation;
d. sovereign industrial capability;
e. operational utility;
f. privacy and civil liberties; and
g. the legitimate use of uncrewed systems across commercial, industrial and recreational sectors.

1.1.2 The overwhelming majority of uncrewed system operations within Australia are lawful and support valuable commercial, industrial, emergency service and recreational activities. Future reforms should therefore remain proportionate to operational risk and avoid imposing unnecessary burden on low-risk operators or emerging Australian industry participants.

1.1.3 The regulatory framework should remain adaptable to emerging technologies including AI-enabled autonomy, autonomous swarming, collaborative uncrewed operations and increasingly software-defined payloads, communications and navigation systems.

1.1.4 For the purpose of this submission, 'Uncrewed Systems (UxS)' refers collectively to aerial, maritime, surface and land-based uncrewed systems, including:

a. Uncrewed Aerial Systems (UAS);
b. Uncrewed Surface Vessels (USV); and
c. Uncrewed Underwater Vehicles (UUV).

1.2 About the Respondents

1.2.1 This submission has been jointly prepared by JVAT and SNC AUS.

a. JVAT is an Australian-owned systems integration and advisory business supporting Defence, government and critical infrastructure sectors across complex operational and regulated environments.
b. SNC AUS provides access to operationally proven sensing, electronic warfare, uncrewed systems and counter-uncrewed systems technologies supporting allied government and Defence customers.

1.2.2 The perspectives presented in this submission are informed by operational, engineering, integration, assurance and regulatory experience across aviation, maritime, critical infrastructure and counter-uncrewed systems environments.

1.3 Scope and Guiding Principles

1.3.1 The Department of Home Affairs Drone Security Consultation Paper [Reference A] outlines proposed approaches to strengthening Australia's national framework for uncrewed systems security. The consultation adopts a risk-based, technology-neutral and principles-driven approach to balancing safety, security, innovation and operational utility while improving detection, identification, enforcement and protection of sensitive sites and public spaces.

1.3.2 This submission addresses the questions posed in the Consultation Paper under the thematic headings used by the Department of Home Affairs. Responses aim to reflect combined operational, technical, integration and governance perspectives relating to uncrewed systems detection, identification, mitigation, assurance and regulatory coordination.

1.3.3 Regulatory obligations and operational controls should remain proportionate to the capability, operating environment and risk profile of the relevant uncrewed system activity. Future reforms should support continued innovation, sovereign industrial capability and responsible adoption while ensuring that higher-risk capabilities and operating environments are subject to appropriate safeguards, oversight and accountability mechanisms.

1.3.4 Counter-uncrewed system activities should follow a graduated and proportionate hierarchy of response comprising:

a. detection;
b. location;
c. identification;
d. tracking;
e. assessment;
f. coordination;
g. mitigation; and
h. investigation.

1.3.5 Active mitigation measures should remain tightly controlled, risk-informed and subject to clear legal authority and operational oversight.

1.4 National Regulatory Coordination and Legal Considerations

1.4.1 Australia's current regulatory arrangements for uncrewed systems are largely organised by operational domain and legislative function, including aviation safety, maritime safety, radio communications, critical infrastructure protection, privacy and law enforcement authorities. As uncrewed systems increasingly operate across and between these domains, there is growing potential for regulatory overlap, uncertainty and inconsistent operational responses.

1.4.2 This challenge is particularly pronounced where systems:

a. operate across air, maritime and land environments;
b. utilise shared radio frequency spectrum;
c. involve autonomous or beyond-visual-line-of-sight operations;
d. interact with critical infrastructure; or
e. create simultaneous safety, security and privacy considerations.

1.4.3 Future frameworks should recognise that safety regulation and security regulation, while closely related, may require different authorities, operational responses and risk tolerances.

1.4.4 Future reforms should prioritise risk-based and nationally coordinated governance arrangements, harmonised regulatory principles and clearly defined operational responsibilities across Commonwealth, State and Territory agencies. This does not necessarily require the establishment of a single regulator, but rather a coherent national framework that clarifies:

a. lead-agency responsibilities;
b. escalation pathways;
c. information-sharing arrangements;
d. operational authorities;
e. evidentiary requirements; and
f. accountability mechanisms.

1.4.5 Many counter-uncrewed system activities, including RF disruption, protocol takeover, GNSS interference, signal interception, forced landing or kinetic defeat, may interact with existing Commonwealth and State legislation relating to:

a. Radio communications;
b. telecommunications;
c. aviation safety;

d. surveillance;
e. privacy;
f. criminal law; and
g. property rights.

1.4.6 Future reforms should therefore establish clear statutory authorities governing:
a. who may lawfully deploy counter-uncrewed system measures;
b. under what operational circumstances;
c. using which approved technologies; and
d. subject to what safeguards, oversight and accountability mechanisms.

1.4.7 Any future framework should clearly distinguish between:
a. passive detection;
b. active detection;
c. electronic disruption;
d. cyber or protocol-based control;
e. physical interdiction; and
f. destructive defeat measures,

1.4.8 with escalating approval thresholds and operational safeguards applied according to risk and consequence.

1.4.9 The framework should also clarify liability, indemnity and evidentiary responsibilities where authorised counter-uncrewed system activities unintentionally affect:
a. third parties;
b. communications systems;
c. aviation operations;
d. emergency services;
e. critical infrastructure; or
f. privately owned platforms.

1.4.10 Expanded authorities should remain proportionate, necessary and subject to appropriate oversight, auditability, data governance and privacy protections to maintain public confidence and legitimacy.

1.4.11 A nationally coordinated approach will support public safety and national security outcomes while minimising unnecessary burden on legitimate commercial, research & development and recreational operators while supporting innovation and sovereign Australian capability development.

2 Proactive Management of Emerging Drone Threats

2.1 Question 1

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

2.1.1 A holistic, all-domain approach to uncrewed system security is appropriate, given that uncrewed systems increasingly operate across aviation, maritime, land, cyber and RF environments simultaneously. This creates operational and regulatory overlap that may not be adequately addressed by domain-specific regulatory structures alone. Within that framework, Uncrewed Undersea Vehicles (UUVs) should be recognised as a distinct capability class due to the unique challenges associated with detecting, tracking, attributing and defeating them. Unlike aerial or land-based drones, UUVs operate in an environment where traditional surveillance, communications and response mechanisms are significantly degraded. Their low observability, ability to operate covertly over long durations and the complexity of underwater sensing make them among the most difficult uncrewed threats to detect and subsequently counter effectively.

2.1.2 Across the broader uncrewed systems landscape, maritime and land-based threats can generally be attributed to one of the listed categories below, based on their intended effect. These include:

a. Intelligence, Surveillance and Reconnaissance (ISR) activities, designed to collect sensitive information;

b. Seaway denial operations intended to interfere with transport, logistics or essential services; and

c. Kinetic, Electronic Warfare threats and potential disbursement of gas/chemical agent release directed against people, infrastructure or critical assets.

The appropriate response should therefore be threat-based and proportionate, shaped by the potential consequences to public safety, economic continuity and national security.

2.1.3 In the maritime domain, Australia faces a particularly significant vulnerability around offshore critical infrastructure, especially oil and gas facilities located within the Australian Exclusive Economic Zone (EEZ). These assets are geographically wide-spread and essential to sovereign energy security, supply chains and broader economic resilience. However, they remain exposed to emerging drone threats, including long-range Uncrewed Surface Vessels (USVs), sub-surface UUVs or commercially available drones launched from civilian vessels. Even relatively unsophisticated actors can pose credible threats to disruption and denial of offshore infrastructure, maritime logistics and port access, with significant economic consequences.

2.1.4 Current regulatory and operational arrangements appear fragmented, particularly for maritime drones. It is understood that the Australian Maritime Safety Authority (AMSA) addresses UUVs and USVs through broader maritime safety and navigation legislation rather than a dedicated regulatory security framework. This creates potential gaps in governance, detection responsibility and operational response authorities where existing doctrine does not provide a clear direction.

2.1.5 Given the strategic implications, Australia should adopt a more proactive posture that not only protects critical offshore infrastructure, but also visibly demonstrates that these assets are monitored and defended. A credible and publicly understood deterrence framework is likely to be more effective than a purely reactive approach after an incident has occurred.

2.1.6 Land-based drones similarly present risks to population and infrastructure. Collision, disruption or malicious interference with critical infrastructure assets could have immediate and widespread public safety consequences.

2.1.7 The framework should also anticipate increasing levels of autonomy, including AI-enabled navigation, autonomous target recognition, swarming and collaborative machine behaviour, which may reduce reliance on traditional operator attribution and command-link detection methods.

2.2 Question 2

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

2.2.1 Implementation of RF-based counter-uncrewed aerial systems (C-UAS) in Australia requires close coordination with the Australian Communications and Media Authority (ACMA) to ensure that RF countermeasures do not unintentionally disrupt essential communications, navigation systems or other critical infrastructure that depend on radio frequency (RF) spectrum for command, control and operational continuity. This is particularly important given the increasing reliance of critical infrastructure, transport systems and emergency services on RF-enabled technologies.

2.2.2 To support both safe drone integration and effective counter-drone operations, uncrewed systems sold or operated within Australia (outside of National Security users) should be required to comply with nationally defined technical RF spectrum usage and cyber assurance standards. These standards should seek to minimise interference with other RF spectrum users, improve interoperability and make drone systems more resilient against tampering, cyber compromise or hostile takeover by malicious actors.

2.2.3 A mode-agnostic, technology-neutral regulatory framework is the most effective approach for managing emerging uncrewed system threats. In this context, ‘mode-agnostic’ means that security requirements apply consistently whether a system is operated manually, remotely or autonomously through onboard software. Rather than prescribing specific technologies, the framework should focus on operational outcomes, risk thresholds and performance-based requirements.

2.2.4

2.2.5 Mitigation measures should be applied proportionately and according to risk. Active counter-drone capabilities such as jamming, spoofing or kinetic interdiction should only be authorised in environments where risks to people, aviation, critical infrastructure or national security exceed clearly defined thresholds; such as airports, ports, military facilities and major public venues. In lower-risk environments, detection, monitoring and reporting mechanisms are generally sufficient and impose far less burden on legitimate operators.

2.2.6 A clear distinction should therefore exist between detection and mitigation, and future frameworks should also address cyber security risks associated with uncrewed systems, including firmware integrity, secure software update mechanisms, supply-chain assurance, spoofing resistance, encryption standards and trusted communications architectures. Detection technologies, including visual, acoustic and radar-based systems, should be broadly accessible to industry and infrastructure operators under simple reporting arrangements. By contrast, active mitigation capabilities should remain tightly controlled in a manner similar to Military Off The Shelf (MOTS) hardware. Specially authorised government agencies will provide oversight of approvals, operational safeguards, and compliance to operational standards.

2.2.7 Australia could consider development of a nationally recognised Trusted Uncrewed Systems Assurance Framework to support government, emergency services and critical infrastructure operators requiring higher levels of cyber assurance, interoperability and supply-chain confidence.

2.2.8 The framework should also minimise regulatory burden for low-risk recreational and commercial operators through streamlined licensing, registration and incident-reporting requirements. Staged enforcement would further support proportionality, using education and warnings for minor breaches while reserving stronger enforcement and mitigation responses for credible threats or repeated non-compliance.

2.2.9 Finally, the framework should include strong privacy protections, secure handling of operational data and regular consultation between government and industry. Clear public guidance and transparent communication will be essential to maintaining public trust, supporting innovation and ensuring operators understand both their obligations and the rationale behind security measures.

2.3 Question 3

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

2.3.1 Australia could adopt a layered standards framework for uncrewed systems that distinguishes between general civilian uncrewed systems operations and higher-assurance systems authorised for critical government, emergency service and national security functions. Under such an approach, a baseline national standard would apply to all civilian uncrewed systems, covering areas such as RF spectrum compliance, cyber assurance, and personnel safety. Above this, a more stringent government-certified standard could be established for approved law enforcement, Defence and emergency services platforms that must continue operating while withstanding counter-uncrewed system activities.

2.3.2 This could be applied to countering of land and maritime uncrewed systems as well as UAS, noting that C-UAS is a very commonly used term. In this response the realisation is that the all-modes approach also applies to counter uncrewed systems, with UAS being one component of land and maritime uncrewed systems.

2.3.3 This model would enable critical functions such as, first responders and security to operate with some level of immunity to the employment of RF-based countermeasures in high-risk or sensitive environments. For example, emergency service drones supporting bushfire response, disaster relief, police operations or critical infrastructure monitoring may need to operate safely within areas where active C-UAS measures are deployed against unauthorised systems.

2.3.4 A useful precedent exists in the United States Department of Defense ‘Blue UAS’ program, which identifies approved drone platforms that meet defined cyber security, supply chain assurance and operational trustworthiness requirements for military use. A similar Australian framework could provide a recognised category of trusted or government-approved uncrewed systems that are subject

to enhanced assurance standards and integrated into national security and emergency response architectures.

2.3.5 Such a framework could also support more sophisticated risk-based geo-fencing and countermeasure policies around sensitive sites and restricted areas. Under this approach, non-approved classes of uncrewed systems operating near sensitive environments can be identified as higher-risk and therefore subject to earlier detection, disruption or denial measures at greater stand-off distances. Conversely, approved high-assurance systems could be permitted to operate closer to restricted boundaries, with countermeasures only triggered if those systems breached defined no-go zones or failed identification and authorisation checks.

2.3.6 This approach would strengthen protection of sensitive infrastructure while preserving operational freedom for trusted government and emergency response operators. It would also incentivise industry uptake of higher cyber assurance and interoperability standards, improve public confidence and create clearer differentiation between legitimate and potentially malicious drone activity in sensitive operational environments.

2.3.7 Table 1 shown below provides a summary of the sectors which might be disproportionately affected by an all-modes approach to drone security.

Table 1. Summary of sectors that could be disproportionately affected by all-modes security measures

Sector	Why it may be disproportionately affected	Government-led mitigation actions
Aviation (airports, airspace air traffic management)	Airports are the most obvious high-risk sites; all-mode detection/mitigation may require costly upgrades and operational changes.	• Prioritise risk-based deployment: only high-risk zones get active mitigation. • Offer technical assistance and funding for detection-only solutions.
Transport & logistics (ports, rail, road)	Ports and rail yards often lack existing detection infrastructure; adding full-scale mitigation could disrupt operations and impose additional costs.	• Provide a phased implementation schedule • Create a “transport-sector exemption” for low-risk zones, with mandatory reporting instead of mitigation.
Critical infrastructure (energy, water, gas, fuel depots, Defence, communications and sensitive sites)	These sites are high-value targets; all-mode mitigation could be essential but also expensive.	• Grant targeted subsidies or tax incentives for installing detection/mitigation. Defence or Australian Protective Services (APS) to be responsible for own infrastructure. • Develop a sector-specific compliance checklist.
Maritime (Port infrastructure, shipping lanes, offshore platforms)	Water-based drones can be harder to detect; all-mode mitigation may be impractical at sea.	• Encourage the use of surface-based detection (radar, acoustic) and a reporting framework. • Coordinate with AMSA for sector-specific guidance if available.
Recreational and commercial operators	Broad all-mode mandates could impose heavy regulatory and financial burdens on hobbyists, businesses and commercial operators. It may stifle innovation which would impact development of sovereign capabilities.	• Maintain a lightweight “report-and-detect” regime. Offer access to designated “test” areas for R&D. • Offer clear, low-cost compliance tools and educational resources.
Urban communities (public spaces, events)	Large gatherings may trigger mitigation that could interfere with normal activities.	• Use risk-based thresholds (e.g., crowd density, proximity to critical assets). • Provide a public-sector reporting portal and clear incident-response protocols.

2.3.8 By combining risk-based deployment, sector-specific exemptions, and targeted support, the government can protect public safety and critical assets without unduly burdening legitimate commercial and recreational drone users.

2.3.9 A phased implementation model should be considered to minimise regulatory burden and allow industry adaptation, commencing with voluntary standards and high-risk sectors before broader implementation. Categories of uncrewed systems correlating to their privileges and requirements helps protect low-cost systems used by hobbyists and innovators from over-bearing regulations required for more privileged operation.

3 Strengthened Counter-Drone Capabilities to Protect the Community and Infrastructure

3.1 Question 4

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

3.1.1 Safeguards and regulatory oversight can be achieved through a combination of measures and controls comprising those that are outlined below:

3.1.2 Counter-uncrewed system responses should follow a proportionate hierarchy of response comprising detection, locating identification, tracking, assessment, coordination, mitigation and investigation activities.

a. Align requirements (registration, detection, countermeasures) with sector-specific risk profiles and operational contexts.

b. Draw on Federal Aviation Administration (FAA) principles for context-driven deployment of detection and mitigation as outlined in [References B–E].

3.1.3 Exemptions or Adjusted Requirements:

a. Provide tailored exemptions or reduced compliance obligations for low-risk operators (e.g., small agricultural, recreational drones operating in uncontrolled airspace, or civil development systems supporting sovereign Defence programs).

b. Allow for flexible, temporary waivers for emergency services and critical response activities.

3.1.4 Government Support and Cost Sharing:

a. Offer grants, technical assistance, or shared infrastructure (e.g., detection networks) for sectors facing high compliance costs (critical infrastructure, small operators).

b. Facilitate financial support for deployment of detection and mitigation technologies.

3.1.5 Clear Guidance and Stakeholder Engagement:

a. Develop sector-specific guidance and education materials to clarify obligations and support compliance. This is particularly important for hobbyist and recreational drone operations.

b. Engage with affected sectors to refine rules and ensure proportionality.

3.1.6 Safeguards for Counter-Drone Measures:

a. Restrict deployment of disruptive counter-drone technologies (e.g., RF jamming or spoofing) to authorised and approved operators in high-risk environments, with oversight of the technologies and safeguards to prevent collateral impacts.

b. Encourage adoption of non-interfering detection and mitigation technologies where possible.

3.1.7 Data Sharing and Incident Reporting:

a. Establish clear, proportionate reporting obligations, with streamlined processes for sectors with limited resources.

b. Protect sensitive sectoral data and ensure information sharing is secure and appropriately limited.

3.1.8 Many counter-uncrewed system activities, including RF disruption, protocol takeover, GNSS interference, signal interception, forced landing or kinetic defeat, may interact with existing Commonwealth and State legislation relating to radio communications, telecommunications, aviation safety, surveillance, privacy, criminal law and property rights. Future reforms should therefore establish clear statutory authorities governing who may lawfully deploy counter-uncrewed

system measures, under what circumstances and subject to what safeguards, oversight and accountability mechanisms.

3.1.9 Any future framework should clearly distinguish between: passive detection, active detection, electronic disruption, cyber or protocol-based control, physical interdiction and destructive defeat measures, with escalating approval thresholds and operational safeguards applied according to risk and consequence.

3.1.10 The framework should also clarify liability, indemnity and evidentiary responsibilities where authorised counter-uncrewed system activities unintentionally affect third parties, communications systems, aviation operations or privately owned platforms.

3.1.11 Expanded authorities should remain proportionate, necessary and subject to appropriate oversight, auditability, data governance and privacy protections to maintain public confidence and legitimacy.

3.2 Question 5

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

3.2.1 Authorisation to deploy counter-uncrewed system technologies should be limited to appropriately authorised Commonwealth and State government entities, approved emergency service organisations and accredited operators operating under defined statutory authority, training and oversight arrangements.

3.2.2 Australia should adopt a tiered authorisation framework that clearly distinguishes between drone detection and counter-drone mitigation. Detection technologies support situational awareness, reporting and response coordination, whereas mitigation technologies can disrupt, disable, redirect or destroy a drone and therefore carry significantly greater legal, safety and operational risk. A distinction should be maintained between passive detection capabilities, which primarily support situational awareness and reporting, and active mitigation capabilities, which may interfere with communications systems, aircraft control or public safety. The authorisation model should reflect that difference.

3.2.3 Active counter-drone mitigation powers could be limited to a narrow class of government-authorised entities with express statutory authority, specialised training, certified equipment and strong oversight. This could include relevant Commonwealth agencies and, where justified, specifically designated State and Territory authorities operating under approved protocols. Control measures such as jamming, Global Navigation Satellite System (GNSS) interference, protocol takeover or physical interdiction can inherently create further risks to aviation safety, communications systems, navigation services, public safety and third parties. For that reason, mitigation capabilities should not be available as a general operational power to private entities or site operators.

3.2.4 This approach is generally consistent with the FAA position, which supports broader identification and reporting arrangements, but states that it does not support C-UAS mitigation by entities other than federal departments with explicit statutory authority. FAA guidance [References B–E] also emphasises that airport environments are especially sensitive and that mitigation can introduce undesirable safety and efficiency impacts.

3.2.5 By contrast, approved detection technologies should be available to a broader but still controlled group of users, including airport operators, critical infrastructure operators, port operators, corrections authorities, emergency services, major event organisers and selected government facilities. This would improve early warning and support timely reporting and escalation, without conferring coercive powers. Within this category, Australia should distinguish between active and passive detection tools, which are generally lower risk, and more intrusive or technically complex detection systems, which should require higher approval thresholds.

3.2.6 It should be noted that in contrast to the FAA, Australia does not require use of Remote ID reception and reporting tools. Australia could consider a nationally harmonised accreditation and certification framework for approved counter-uncrewed system operators to ensure consistent competency, governance and operational accountability. FAA guidance describes Remote ID as foundational to drone safety and security because it helps authorities and law enforcement identify a drone and locate the control station when a drone appears to be flying unsafely or unlawfully. This is a significant difference, and this should be factored into the proposed authorisation framework.

3.3 Question 6

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

3.3.1 Where operators are not appropriately security-clearance vetted, a state-sponsored actor or extremist could infiltrate security companies contracted to support major public events and, from inside, disable the C-UAS system to support hostile acts.

3.3.2 Any expansion of counter-drone powers in Australia should be approached with significant caution. While there is a legitimate need to respond to malicious or unsafe drone activity, expanded counter-drone measures create substantial risks if they are introduced too broadly, without clear legal authority, technical safeguards, operator competency standards and strong oversight. The key concern is not only whether additional powers are needed, but who should hold them, under what conditions, and with what accountability mechanisms.

3.3.3 The main concerns are:

a. Aviation safety and critical infrastructure risks - The most significant concern is the potential for counter-drone measures to create unintended risks to civil aviation safety. Although airports, ports, prisons and critical infrastructure may have the strongest case for enhanced powers, they are also fragile environments where introduced counter-drone measures can inadvertently present catastrophic consequences.

b. Radio frequency and communications interference - Many counter-drone technologies rely on disrupting or interacting with radio frequency signals such as critical communications and navigation systems. The risks and implications of this are heavily context dependent, i.e., within proximity to fuel, explosive ordnance or people.

c. Public safety and physical harm - Measures that disable, redirect or kinetically defeat drones may cause the aircraft to crash, fall unpredictably or be diverted into people, vehicles, buildings or critical assets.

3.3.4 With legal uncertainty and overlap of existing laws, expanded counter-drone powers may create legal complexity across:

a. aviation law;

b. telecommunications and radio communications law;

c. privacy and surveillance law;

d. criminal law;

e. evidence and investigatory powers; and

f. state and federal jurisdictional boundaries.

3.3.5 Decision-making counter-drone technologies require a full understanding of operational environments and risks. Sustainment and training of the tool are critical to the capability.

3.3.6 Where operational responsibilities intersect between aviation, radio communications, telecommunications, criminal or privacy legislation, a lead-agency model supported by pre-defined escalation and coordination arrangements should apply.

3.3.7 Impacts on legitimate drone use and innovation - Australia has a growing legitimate drone sector across Defence, infrastructure, agriculture, logistics, emergency response, media and surveying. This sector requires space to safely exist without undue threat of counter-drone measures.

3.3.8 Privacy and civil liberties concerns - Some detection and counter-drone systems may collect or process information about devices, communications, locations or individuals.

3.4 Question 7

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

3.4.1 The public could have a help line to call, or instant messaging service available (in addition to 000), to communicate suspicious operation or potential threats. This said, every uncrewed system they see operating may not be for malicious purposes. Australia should consider a nationally interoperable reporting architecture capable of securely routing incidents between relevant agencies, including

CASA, Home Affairs, State Police, Defence and critical infrastructure operators. The public could be able to share pictures taken on their mobile devices for law enforcement/first responder type mapping applications to immediately slew to an area surrounding the location based on reading the associated imagery geo-location metadata as discussed below.

3.4.2 Other measures that could be employed to identify emerging drone threats are shown in Table 2.

Table 2. Potential Identification of Emerging Drone Threats

Category	Details
Active participation in detection and reporting	• Industry operators (airports, ports, critical infrastructure, event organisers, emergency services, commercial drone users) should be authorised to deploy approved detection technologies (optical, acoustic, radar). • Industry operators should report any suspicious or non-compliant drone activity to the designated national counter-drone hub or the Australian Civil Aviation Safety Authority (CASA) in a timely, structured manner.
Structured reporting framework	• A clear, single-point reporting portal should be provided, accepting incident details, location, drone identification, operator contact (if known) and any supporting evidence (video, audio, sensor data). • Reports should be automatically routed to the appropriate authorities (CASA, Australian Defence Force, APS, Australian Security Intelligence Organisation) for assessment and action.
Data sharing under strict privacy safeguards	• Industry and public reports should be shared only with the agencies that have the legal authority to investigate and, if necessary, take mitigation action. • All data handling must comply with the Privacy Act, the Telecommunications Act and relevant Civil Aviation Act, ensuring that personal information is protected and retained only as long as required for investigation.
Training and awareness	• Industry stakeholders should receive regular training on how to recognise potential threats, how to operate detection equipment safely, and how to complete the reporting process accurately. • Public awareness campaigns (e.g., “Know the signs of unauthorised drone activity”) can encourage citizens to report suspicious activity without encouraging panic or unnecessary interference.
Collaboration with government agencies	• Domestic and international industry should collaborate with CASA, the Australian Defence Force (ADF) and the Australian Security Intelligence Organisation (ASIO) to share best practices, threat intelligence and emerging risk profiles. • Public-sector partnerships (e.g., local councils, transport operators) should be encouraged to create a coordinated national network of detection and reporting.
Clear boundaries for public action	• The public should be advised that while they can report suspicious activity, they must not attempt to intervene or deploy counter-drone measures. • Any attempt to jam, disable or otherwise interfere with a drone is illegal unless authorised by a specific government entity under the proposed ‘statutory framework’.
Feedback loop and continuous improvement	• Reports that lead to confirmed threats or incidents should be fed back to industry and the public to refine detection criteria, update training materials and improve reporting tools. • Periodic reviews of the reporting system will ensure it remains effective, user-friendly and aligned with evolving threat landscapes.

4 Enhanced Identification and Tracking Through Electronic Conspicuity

4.1 Question 8

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?

4.1.1 No single identification technology is likely to provide sufficient coverage across all operating environments. A layered model incorporating Remote ID, RF detection, radar, electro-optical sensing and operator attribution mechanisms may provide greater resilience and operational flexibility. Along with comments relating to mandating standardisation, tools that could be implemented to support real-time visibility of drones are:

a. A system similar to COSPAS SARSAT (international, satellite-based Search And Rescue (SAR) system), supported by national regulation bodies;

b. Implementation of a unique hexadecimal coded signal as per example embedded within Personal Locator Beacon (PLB);

c. Emergency Position Indicating Radio Beacon (EPIRB); and

d. Emergency Locator Transmitter (ELT) devices

4.1.2 The COSPAS SARSAT beacon devices require registration of a user, platform as well as a next of kin. This type of capability could be standardised and mandated for commercial uncrewed systems operating in Australia, enabling law enforcement to conduct checks when uncrewed systems are operating in sensitive areas/suspicious manner. This would be a prescribed requirement for proposed categories of drones that can fly even remotely close to sensitive sites and infrastructure. This ensures unidentifiable or unauthorised drones cannot surveil sites such as Defence sites from a stand-off distance with advanced optical hardware without requiring some sort of identification measure.

4.1.3 Countering UAS is a primary task. However, where authorised under legislation, federal and state law enforcement should be able to support lawful attribution and operational response activities, including geo-location of the uncrewed system and, where appropriate, correlation with available CCTV to assist with identification of malicious actor type users.

4.1.4 A friendly UAS operating in conjunction with the C-UAS system could be employed responding to detected locations, to support lawful attribution, evidentiary collection and investigative processes where authorised under legislation, cueing law enforcement to investigate as appropriate.

4.1.5 The Australian Government's Drone Security Consultation Paper recommends a risk-based, context-driven approach which is similar to FAA's guidance but adapted to Australian conditions. However, unlike the FAA, there are no requirements for Remote ID functionality in Australia. Therefore, key visibility elements for airborne drone location, altitude and operator attribution cannot be directly measured or recorded. In the absence of Remote ID there are alternatives that can be deployed as shown in Table 3.

Table 3. Alternatives to real time visibility not using Remote ID functionality

Alternative	Strengths	Typical Use-Case	Notes
Radar Detection	No need for drone cooperation; works in all weather. Detects, locates and tracks – including non-RF emitting systems	Airports, offshore platforms, critical infrastructure.	Requires line-of-sight; limited altitude resolution. Pending radar type/capability can track hundreds whilst still searching for others. Can cue a RF system to ascertain communications method and subsequently employ appropriate technique to counter (with suitably sophisticated solution).
RF Detection	Can identify the controller without GPS data.	High-risk zones where operator	Works best with a curated database of known controller signatures.

Alternative	Strengths	Typical Use-Case	Notes
	Can detect both uncrewed system and control location (pending clear LOS detection).	attribution is critical.	Pending sophistication of system, can timestamp and record historically over time of initial detection to where the uncrewed system eventuated from, what route it took and where the GCS is located. If fitted with such capability, could receive registered UAS location and user POC information.
Visual EO/Infrared	EO/IR provides drone type and size classification which can be augmented with vision-based methods.	Urban events, high-risk sites with visual access.	Requires clear line-of-sight and can be affected by lighting. Can employ automatic identification type AI algorithmic software processing to assist with identification of uncrewed system type. For integrated systems, optical sensor provides a cue for counter capabilities.
Integrated Sensor Solutions	Combines radar, acoustic, RF, and visual for robust detection.	Airports, critical infrastructure, military sites.	Higher cost but offers the most comprehensive visibility.

4.1.6 These alternatives are initial recommendations and should be tailored based on the specific risk profile of each environment, following the risk-based model laid out in the consultation paper and the FAA's UAS System Detection – Technical Considerations [Reference E]

4.2 Question 9

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?

4.2.1 Any of the above to an appropriate level, so long as they are appropriately security clearance vetted and trained. This technology should be integrated, networked and centrally managed, not kept in stovepipes. The drone detection capability surrounding correctional centres should be integrated into the same system as the critical infrastructure, etc. with each location having only a segregated view to see the area surrounding their zone of influence. This can prevent malicious actors having ease of infiltration. This approach will have a centrally managed picture which could tip and cue individual locations based on the evolving threat.

4.2.2 Australia should extend access to drone detection equipment beyond traditional law enforcement and security agencies to a broader group of authorised operators, particularly emergency services, prison operators, critical infrastructure operators and major event organisers. However, this access should occur within a tightly regulated, risk-based framework with clear training, certification, oversight and data-sharing requirements.

4.2.3 The consultation paper correctly identifies that many of the highest-risk environments are not directly controlled by police or intelligence agencies, but by operators responsible for critical public services and crowded places. These include energy facilities, hospitals, correctional centres, ports, transport hubs and major events. In practice, these organisations are often the first to observe or experience drone incursions and require real-time situational awareness to protect public safety and maintain continuity of operations.

4.2.4 Restricting drone detection capability solely to law enforcement would create operational delays and leave many vulnerable sites dependent on external response times. This is particularly problematic given that drone threats are often fast-moving, low-cost and difficult to attribute. The paper also notes that effective counter-drone responses increasingly depend on real-time detection, tracking and coordinated information sharing between government and infrastructure operators.

4.2.5 The FAA technical guidance supports a measured expansion of detection capability, while highlighting the complexity of operating these systems effectively. Detection technologies require specialised

training, calibration, updating and interpretation to avoid false positives and environmental interference. The guidance also warns that poorly configured RF-based systems may affect communications, navigation systems and other critical infrastructure. This reinforces the need to distinguish between passive detection systems and active counter-drone mitigation capabilities such as jamming or signal interception.

4.2.6 Accordingly, passive detection technologies should be made available to approved non-law-enforcement operators under a licensing and accreditation regime. This could include radar, RF detection and electro-optical systems integrated into existing security operations centres. By contrast, active mitigation capabilities that interfere with the electromagnetic spectrum or take control of aircraft should remain restricted to appropriately authorised government agencies due to their safety, RF spectrum-management and legal implications.

4.2.7 A tiered model therefore offers the best balance between security, proportionality and operational effectiveness. It strengthens national resilience, improves protection of high-risk sites and enables faster local responses, while maintaining appropriate safeguards, oversight and central government coordination.

4.2.8 Approved operators should be subject to common national operating standards, training requirements and reporting obligations to ensure consistency across jurisdictions.

4.3 Question 10

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?

4.3.1 Registration and identification obligations should be proportionate to operational risk, including factors such as payload capability, autonomy, endurance, beyond-visual-line-of-sight operation and proximity to sensitive infrastructure. Registration and enhanced identification requirements should move beyond the current commercial-only model and adopt a risk-based approach focused on capability, operational environment and potential security impact, rather than solely the purpose of use.

4.3.2 At a minimum, all aerial drones above a defined weight, range or payload threshold should be subject to mandatory registration regardless of whether they are used commercially, recreationally or by government agencies. Drones air, land or sea based, capable of beyond visual line of sight operation, autonomous navigation, high-resolution sensing, payload carriage or operation near sensitive infrastructure should also require enhanced identification measures. These attributes while common in drone platforms can be characteristic of ISR assets capable of gathering sensitive data such as signals or communications.

4.3.3 Enhanced electronic conspicuity and identification requirements should apply to drones operating near airports, ports, correctional facilities, energy infrastructure, defence establishments, major public events and emergency response zones. This should include remote identification capability, operator attribution and real-time location reporting accessible to authorised agencies and critical infrastructure operators.

4.3.4 A tiered framework should also recognise trusted or government-assured platforms, particularly for law enforcement, emergency services and critical infrastructure operators. These systems could operate under enhanced authorisations where they comply with higher cyber assurance, interoperability and operational safety standards.

4.3.5 Low-risk recreational users operating lightweight drones in uncontrolled airspace or designated areas should remain subject to proportionate and streamlined requirements to avoid unnecessary regulatory burden. However, even low-cost consumer drones can present surveillance, disruption or safety risks when operated irresponsibly or maliciously. Accordingly, a baseline registration requirement linked to operator identity should still be considered for most powered aerial drones capable of operating beyond short-range recreational use.

4.3.6 Finally, any registration and identification framework should be interoperable nationally, digitally accessible and designed to support future expansion across maritime and land-based uncrewed systems as those technologies become more widely adopted.

4.4 Question 11

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

4.4.1 A government-sponsored, very small form-factor electronic identification capability; whether modelled on the COSPAS-SARSAT method referenced above, or an equivalent self-reporting beacon technology should be developed, noting that any such approach depends on continuous GNSS availability. Additional technologies may include cryptographic identity verification, secure beaconing architectures, digital certificates and trusted telemetry frameworks capable of supporting secure operator and platform authentication.

5 Balanced Enforcement That Deters Misuse and Enables Innovation

5.1 Question 12

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

5.1.1 Enforcement frameworks should distinguish between accidental non-compliance, negligence, recklessness and deliberate hostile activity, with penalties scaled according to intent, consequence and repeat offending. The most effective deterrence framework would combine proportionate penalties with credible operational consequences and visible enforcement. A graduated model should apply, distinguishing between accidental non-compliance, reckless behaviour and deliberate malicious activity near sensitive locations such as airports, ports, correctional facilities, defence establishments and critical infrastructure.

5.1.2 Minor or first-time infringements should attract education notices or moderate fines, while repeated breaches, intentional incursions or operations creating safety or security risks should attract substantial financial penalties, licence suspension, equipment seizure and potential criminal prosecution. In serious cases where there is a provable intent to cause harm to estate, personnel, or threaten/degrade national security, criminal prosecution in line with conventional weapons or espionage may be warranted.

5.1.3 Dedicated RF-based counter-drone defeat capabilities at sensitive locations could provide an immediate operational response to unauthorised drone activity, including forcing drones to land safely within controlled recovery zones. This creates a direct consequence for operators regardless of police response times or competing operational priorities.

5.1.4 To reinforce deterrence, drones intercepted within restricted zones should be subject to seizure, forensic analysis and evidentiary retention to support investigations and enforcement actions. Public awareness of these consequences, combined with visible enforcement activity, would significantly strengthen deterrence while remaining fair and proportionate to the level of risk and intent involved.

5.2 Question 13

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?

5.2.1 A nationally standardised incident taxonomy and data-sharing framework would support trend analysis, intelligence fusion and operational coordination across jurisdictions. Reporting obligations for abnormal or unauthorised drone activity should be risk-based, streamlined and nationally interoperable. Critical infrastructure operators, airports, ports, correctional centres, emergency services and major event organisers should be required to report significant drone incidents where there is a suspected threat to public safety, operational continuity, national security or restricted areas.

5.2.2 The reporting process should be simplified, time-efficient and supported through standardised digital reporting tools. Information should initially flow into state or territory-level databases, with automated replication into a secure national database to support trend analysis, intelligence fusion and future investigations. This would allow incidents to be recalled, correlated and analysed across jurisdictions where patterns of malicious or coordinated activity emerge.

5.2.3 A centrally coordinated operational reporting framework would significantly improve situational awareness and reduce duplication between agencies. Reports should include basic but actionable information such as time, location, drone description, flight profiles, captured imagery or sensor data and whether the activity involved restricted infrastructure or controlled airspace incursions.

5.2.4 Regular intelligence briefings and information-sharing arrangements between relevant agencies should also be established. This would support Defence, State and Federal Police, Customs, Border Force and critical infrastructure stakeholders by improving threat awareness, identifying recurring actors or methods and strengthening coordinated operational responses across all domains.

6 Drone Classifications and Operating Restrictions

6.1 Question 14

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

6.1.1 A distinction should exist between permanent prohibited-use zones, temporary operational exclusion zones and enhanced-monitoring areas where detection and reporting capabilities are prioritised. Specific no-use and enhanced-monitoring zones should be designated around sensitive and high-consequence locations including hospitals, correctional centres, energy infrastructure, airports, ports, Defence establishments and major public venues. These areas should be continuously monitored and integrated into centrally coordinated operational networks, likely at a State or regional level depending on geographic coverage requirements. These no-use type areas should be well publicised and perhaps available electronically as overlays that uncrewed systems operators can download to their mapping application graphic user interface (GUI) devices to ensure they have a geographical representation for indication of where to keep their uncrewed systems external of the boundary to the no-use area. These could be centrally and nationally managed for one stop shop access.

6.1.2 Enhanced-monitoring zones should employ RF-based counter-uncrewed aerial system capabilities specifically engineered to operate safely within complex and sensitive RF environments such as hospitals, emergency services networks and critical infrastructure facilities. A risk-based framework should allow monitoring, detection and proportionate response measures tailored to the operational sensitivity and threat profile of each location.

6.1.3 A staged approach to approved drone operation and proximity to these zones should be dependent on the registered category of the drone. This ensures those with a recognised use case can operate under an identified and approved status within the monitored zone without posing a threat. Those in less regulated categories can still operate but at an approved distance removed from the monitored zone. Future frameworks should support dynamic geo-fencing and machine-readable restriction data capable of integration into commercial drone operating systems and operator applications.

6.2 Question 15

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

6.2.1 Drone operations should be completely restricted, unless specifically authorised, around critical infrastructure and sensitive government or security-related locations where disruption, surveillance or attack could significantly impact public safety, national security or economic continuity.

6.2.2 Zones that should be completely restricted include:

a. Specific Infrastructure - Water supply/treatment facilities, power generation/transformer facilities, power lines, gas infrastructure, and selected hazardous industrial, fuel storage and

energy infrastructure assessed as high consequence under a risk-based framework, including oil rigs; and

b. Specific Entities - Airports, law enforcement premises, government buildings and sites, Defence buildings and sites, prisons, port/wharf areas, hospitals, embassies, local and state policing and emergency service responders.

6.2.3 Each of these locations can have a detrimental effect on the general public sentiment and need to be protected.

6.2.4 Government designation will be the initial and primary means of granting exclusion zones. In addition to that, industry and the broader public should have an available mechanism to propose an exclusion zone with a justified case. This could be for industrial manufacturing or testing facilities where Defence related technologies could be observed.

6.3 Question 16

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

6.3.1 Two primary means could be enacted to educate / communicate operators on no-drone-zones. Firstly, where operators are required to hold a license to operate the drone, training and resources provided to confer the risk and consequences of no-drone-zones and where to find them. Secondly, media campaigns similar to 'Dial Before You Dig' to educate recreational users of the risks and importance of checking their operating space prior.

6.3.2 Signposting at and surrounding sites or areas, supported by publication in applicable brochures available to the public, is recommended. For maritime environment have these promulgated in national nautical charts, notices to mariners (NTM), and state-based boating brochures/pamphlets. Restricted areas for no-fly zones with applicable airspace volumes are published already and activated by Notices to Airmen (NOTAMs), but perhaps these need to be reviewed to include 24/7 regulations on UAS without prior flight planning/authorisation. These type areas should be well publicised and perhaps available electronically as overlays that uncrewed systems operators can download to their electronic mapping/nautical chart applications for use at uncrewed system control station to ensure operators have a geographical representation for indication of where to keep their uncrewed systems external of the boundary to these areas. These should be centrally and nationally managed for one stop shop access.

6.3.3 Minimum operator awareness, registration and onboarding requirements proportionate to operational risk should apply. This could include a computer-based training and test to ensure a basic understanding of obligations, restricted zones and safe operating practices.

7 Build Public and Industry Awareness

7.1 Question 17

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

7.1.1 Public communication should reinforce that reforms are intended to balance innovation, safety, privacy and national security outcomes while supporting responsible use of uncrewed systems. Public education should focus on practical, real-world examples of how drones can unintentionally or deliberately create safety, security and economic risks across all domains. This includes risks to aircraft, emergency operations, ports, offshore infrastructure, correctional facilities and crowded public spaces. Information should explain how even small recreational systems can interfere with critical infrastructure, disrupt transport networks or compromise privacy and security.

7.1.2 Education should also improve awareness of cyber and RF-related risks, including how drones can be tampered with, spoofed or used for intelligence collection. Clear explanations of restricted zones, no-go areas, reporting obligations and penalties for misuse are essential. Education material should also improve awareness of cyber and data-security risks associated with poorly secured or untrusted uncrewed platforms and supporting software ecosystems. Importantly, messaging should distinguish

between legitimate recreational use and genuinely unsafe or malicious behaviour to maintain public confidence and support responsible drone adoption.

7.1.3 This education piece can also provide information on the public's 'Duty of Care' and provide information on the appropriate ways to report a suspected risk. This provides the public a means of action to then enact if/when needed.

7.2 Question 18

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

7.2.1 Operators would benefit from a nationally integrated digital platform consolidating operational guidance, restricted zones, alerts, reporting obligations and jurisdictional requirements. Operators would benefit most from a single national digital platform that consolidates all drone-related obligations across aerial, maritime and land-based systems. This platform should include interactive maps of restricted zones, real-time alerts, registration services, operating guidance and incident reporting tools.

7.2.2 Mobile applications integrated with geofencing and live airspace volumes or maritime restriction zone updates would significantly improve operator awareness and compliance. Standardised onboarding material at the point of sale, including QR-linked guidance, should also be mandated for retailers and manufacturers.

7.2.3 Industry associations, model aircraft clubs governed by the Model Aircraft Association of Australia (MAAA), maritime groups and commercial operators should be leveraged to distribute consistent guidance. Training resources should be tiered according to operational complexity, ensuring recreational users receive simple, practical guidance while higher-risk operators receive more detailed operational and security education.

7.3 Question 19

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

7.3.1 Public communication should clearly explain why restrictions exist, including aviation safety, RF integrity, emergency response protection and critical infrastructure resilience considerations. The most effective approach would combine real-time digital awareness tools with clear, practical public education campaigns. Operators should have access to simple mobile applications showing live restricted zones, temporary exclusion areas and emergency operation boundaries across air, maritime and land environments. This could be implemented within a Google Earth framework.

7.3.2 Public campaigns should focus on straightforward operational guidance such as 'where you can fly', 'what to avoid' and 'what to do if uncertain'. Visual examples of restricted infrastructure, emergency zones and sensitive locations would improve understanding significantly more than legislative language alone.

7.3.3 Mandatory pre-flight awareness prompts, digital geofencing notifications and simple online refresher modules could further reduce accidental incursions. Public messaging should also clearly explain why restrictions exist, including risks to aircraft safety, emergency response operations, critical infrastructure and public safety, helping operators understand that compliance is a security and safety obligation rather than simply a regulatory requirement.