Australian Government

Drones Security

Public Consultation Paper

April 2026

Contact us

Enquiries regarding the licence and any use of this document are welcome at:
Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

Table of Contents

Executive Summary 2
Introduction 3
Why Australia needs drone security reforms 4
What makes drones a security risk? 5
Policy development areas 7
Proactive management of emerging drone threats 8
Strengthened counter-drone capabilities to protect the community and infrastructure 9
Enhanced identification and tracking through electronic conspicuity 11
Balanced enforcement that deters misuse, and enables innovation 13
Drone classifications and operating restrictions 15
Build public and industry awareness 17
Annexure A: What is a drone? 18
Annexure B: Drone safety and security threats 19

Executive Summary

Drones are now part of everyday life in Australia. They are used by businesses, farmers, emergency services, researchers, creatives, and recreational users, delivering significant economic, environmental, industrial and social benefits. While most people think of drones as uncrewed aircraft, modern drone systems can also operate on land and at sea or in an intermodal context, for example freight hubs. As the technology has advanced, drones have become more affordable, more capable, and easier to operate, accelerating their uptake across the economy. These same characteristics, however, are also changing the security risks of drone misuse.

The rapid growth in drone use increases the likelihood of misuse, accidents, and deliberate harm. Drones operating in the air, on land, or at sea can be used to interfere with critical infrastructure, disrupt essential services, conduct unlawful surveillance, deliver contraband, or operate in restricted areas. Without forward-looking, adaptable policy settings, Australia will face challenges keeping up with an evolving threat landscape. This leaves gaps that malicious actors could exploit, diminishing public safety and national security, while damaging social license for the legitimate use of drone technologies.

Australia's current regulatory framework has largely focused on aviation safety and the integration of aerial drones into controlled airspace. While this approach has supported aviation safety outcomes, it does not effectively support responses to security risks, particularly around critical infrastructure, major events, crowded places, and sensitive sites. Similar risks are also emerging as land based and maritime drones become more widely used.

The Australian Government is therefore considering reforms to strengthen Australia's approach to drone security, with an initial focus on aerial drones, reflecting their accessibility, affordability and risk profile. These reforms are intended to improve the ability to detect, identify, and respond to negligent, dangerous or malicious drone activity, while continuing to support legitimate and innovative uses of drone technology. This includes consideration of improved identification and tracking, appropriate counter drone capabilities for authorised agencies, data sharing, updated enforcement powers, strengthening operating rules in high-risk locations, and targeted education to support responsible drone use.

This consultation seeks views from the public, industry, and other stakeholders on how best to balance safety, security, innovation, and community trust as drone technologies continue to evolve.

Introduction

Uncrewed systems technologies, commonly referred to as drones[1], are rapidly advancing and driving productivity growth across the Australian economy.

Logistics, mining, construction and agricultural sectors are some of the many key industries harnessing drone technologies to unlock new capability and productivity efficiencies. Australian television companies, photographers, hobbyists, and filmmakers have embraced drones to capture imagery that was once impossible or expensive. Governments are encouraging investment in drone technologies to support sovereign capability and economic transition, with increasing use across emergency management, defence, border security, policing, traffic management, and environmental monitoring.

Drone technologies have undergone a remarkable transformation since their inception. Starting as early experiments in using balloons, to the highly capable drones now embedded across military, commercial, and civilian life, drones are now complex cyber-physical systems that are best described as:

- not having a person onboard the device
- autonomously or remotely operated
- moving in the air, on the ground, on water, or under water.

Alongside the opportunities these technologies offer, drones also present security risks and challenges to public safety, critical infrastructure and Australia's sovereignty.

Aerial drones have seen constant innovation driving improvements towards autonomous navigation, object recognition, battery life, and sensor payloads. Advances that enable drones to operate longer, travel further, evade detection, and carry heavier payloads have increased their appeal to those seeking to break the law and undermine Australia's security. This risk is compounded by autonomous operation, swarming capabilities, and growing resistance to mitigation measures, enabling coordinated and adaptive threats that can challenge existing detection and response frameworks.

Drone use in conflicts and grey zone operations overseas continues to blur the line between military and civilian use cases and legitimate activity from careless or malicious use. Governments and industries around the world are changing the way they think about drone security to stay ahead of the changing threat landscape.

The *Aviation White Paper: Towards 2050* (AWP), outlined the Australian Government's vision for aviation for the next 25 years. A key theme in the AWP is to ensure Australia's aviation sector remains safe, secure, competitive, and trusted, particularly as it adapts to new technologies and changing markets.

In recognition of the disruptive nature of aerial drones to aviation, the AWP identified a range of initiatives to support the safe integration of aerial drones into Australia's aviation ecosystem. This also includes consideration of drone security risks, with the Australian Government committing to:

Introduce new legislation by 2030 to protect Australian communities, infrastructure and businesses from security risks of aerial drones and Advanced Air Mobility.

While the AWP is naturally focused on aerial drone technologies, the growing use of other drone technology types across the Australian economy carries many of the same security risks. Against an increasingly challenging global security environment and rapidly advancing drone technology, the Australian Government is seeking to act quickly, recognising the need for urgent reform.

[1] There are many different types of drones in use today, and they are referred to by a wide range of names depending on their design, purpose, or operating environment. To assist with readability this paper will use drones as a catchall for land, sea and air drones, unless otherwise identified as a particular mode type. Annexure A provides a more detailed description of the different types of drones.

This consultation paper seeks the broadest range of views and takes a principles-based approach to ensure Australia's drone security policy reforms appropriately balance safety, security, innovation and community trust while supporting the delivery of related AWP initiatives. While these reforms are intended to apply across all drone systems over time, the initial focus will be on aerial drones. To achieve these objectives, we intend for Australia's drone security framework to:

- be sector agnostic, dealing with aerial drones in the first instance, while also considering land and maritime drones (surface and sub-surface)
- be technology neutral, ensuring readiness for future advances in drone and counter drone technologies
- enable authorised parties to access and use counter-drone technologies, where necessary, to deliver public safety and national security outcomes, subject to appropriate safeguards.
- make sure drones are able to operate in the right places at the right times
- enable drone-related information and data sharing between appropriate agencies
- deter drones misuse, particularly where harm is intended or security impacted, through penalties that complement aviation safety enforcement.

Clear security guardrails that complement existing drone safety settings for emerging technologies will provide greater certainty for users and industry, support broader adoption, and enable continued innovation across Australian society.

For example, any future work on the security of land-based drones would take into consideration regulations applicable to on-road and off-road automated vehicles. This includes the Automated Vehicle Safety Law currently being developed by the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts.

The Australian Government recognises drone-related privacy and noise impacts concern some members of the community. While future security-related measures may have the added benefit of simultaneously mitigating some aspects of privacy and noise concerns, specific consideration of these matters fall outside the scope of the considerations of this consultation.

Why Australia needs drone security reforms

The Australian Government places a high priority on keeping our community safe and secure. This includes protection from negligent, malicious, dangerous or criminal drone operations. Drones are increasingly being misused for harmful activities, including illegal surveillance, smuggling, espionage, and interference with sensitive sites and major events.

Following the unidentified drone operations at the United Kingdom's Gatwick Airport in 2018, the Australian Government has taken an iterative regulatory approach, with the incident serving as a significant catalyst for strengthening existing safety based regulatory measures for aerial drones.

Since then, technologies have evolved and their use expanded, for example, automated land-based devices such as footpath-based delivery devices, domestic devices (e.g. lawn mowers, vacuums), and various agricultural and mining vehicles. Australia's drone security policies and laws need to respond to the contemporary technologies and threat environment to protect the community, our critical infrastructure, complementing aviation safety.

Establishing specific security settings will enable drones to play a productive and safe role and support the integration of drones into Australia's economy. Equally, building public trust in drone technologies gives industry the certainty it needs to continue attract investment, grow jobs and deploy drone technology to seize productivity and growth opportunities across the economy.

What makes drones a security risk?

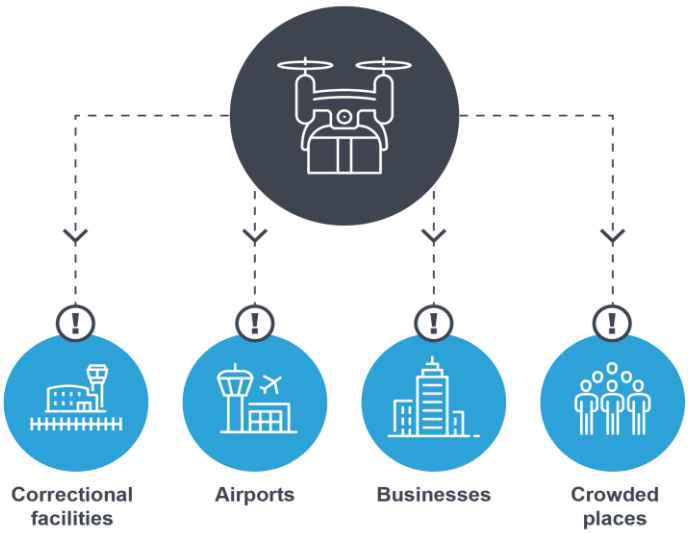
Drones represent a rapidly growing and complex security challenge because they combine accessibility, capability, and anonymity in ways that traditional risk controls cannot easily address. The technologies low cost, ease of accessibility, and minimal skill requirements for users greatly reduce the barrier for misuse. This provides an opportunity for hostile states, criminals, extremists, and negligent operators to exploit drone technology without significant resources or expertise[2]. Like any other cyber-enabled and connected system, drones can also introduce cyber and supply chain security risks for legitimate users.

- ☑ Accessible — easy for anyone to buy, operate, and modify.
- ☑ Capable — able to carry sensors, weapons, and contraband.
- ☑ Hard to detect — small, fast, quiet, and sometimes increasingly autonomous.
- ☑ Hard to attribute — operators stay remote and concealed.
- ☑ Dual use — beneficial tools easily repurposed for harmful acts.
- ☑ Rapidly evolving — technology outpaces current laws and countermeasures.

Operating beyond traditional security boundaries, aerial and sub-surface drones create a complex three-dimensional threat environment for sensitive infrastructure, industry, government, and important cultural and major event sites. Traditional access and perimeter controls such as fences, bollards, standoff zones, and security guards offer limited protection against different types of small, fast, and agile drone platforms.

Drones can also be attractive to criminals or other hostile actors due to their affordability, accessibility, and ability to be operated remotely with limited visibility of the operator. They may be misused for unlawful surveillance, harassment, or interference with public events, and in more serious cases adapted to carry hazardous items or conduct sabotage or attacks against high office holders.

Misuse of drones can pose risks to public safety and national security, including disruption to essential services, interference with critical infrastructure, and impacts on emergency, law enforcement and security agency operations. Such incidents can undermine public confidence in the safe and legitimate use of drone technologies.



[2] Annexure B identifies the diverse range of safety and security threats that may result from the malicious or careless use of drones.

Without updated rules and safeguards, there is a risk that criminals and other hostile actors will increasingly exploit drone technologies. Modern and adaptable policy settings are therefore required to ensure the regulatory framework keeps pace with evolving capabilities and the changing security environment.

Even when drone operators have no malicious intent, careless or unskilled use can lead to accidents, injury, property damage, or unintentional exposure of sensitive information. For aerial drones in particular, as airspace grows more crowded and enforcement becomes challenging, the risks associated with unauthorised or unpredictable drone flights expand.

While all drone types can put critical infrastructure at risk through surveillance or operational interference, aerial drones are increasingly becoming a threat vector. In military and civil contexts, relatively inexpensive drones are used for hostile reconnaissance, targeting, and improvised attacks, demonstrating how quickly consumer technology can be adapted for hostile purposes.

In addition to their potential physical impacts, drones are complex, connected cyber systems that can be exploited by malicious actors. Core components such as navigation, communications, software, and payload systems may be vulnerable to interference or takeover, meaning drones used legitimately could be compromised or controlled by third parties.

Some countries may use national security, intelligence, cybersecurity or data governance laws to compel companies to provide access to data, systems, or technical assistance in support of state objectives, even if those companies operate overseas. These legal obligations can apply to manufacturers and services providers, including those producing or operating drones, sensors, platforms, and associated software of cloud services.

As drones become more autonomous, more networked, and more widely used across civilian, commercial, and governmental contexts, these risks grow in significance. Australia’s policy settings should consider both the security risks of drone misuse. They should also support resilient onboard systems, secure communications and navigation, and effective management of software and firmware over a drone’s lifecycle.

In this context, considering cyber risks as part of drone security reform initiatives supports a more holistic approach to risk management, recognising that modern drone systems rely on interconnected digital technologies that can introduce vulnerabilities beyond the physical domain.

Policy development areas

While all drone types can pose security concerns, this document prioritises the response to aerial drone threats, as they present the most immediate and significant risks due to their accessibility, affordability, and ease of use. The concepts outlined are also intended to inform approaches to other drone modes where practicable.

The areas outlined below provide the structure for this public consultation document.

Proactive management of growing drone threats

Introduction of a national policy framework that anticipates and addresses evolving security risks posed by aerial drones in the first instance, while considering how similar policy approaches could be used to limit threats from surface, sub-surface maritime, and land-based drones.

Strengthened counter-drone capabilities to protect the community and infrastructure

Enhance Australia's capacity to detect, identify, mitigate and counter malicious or unsafe drone activity by expanding counter-drone capabilities and authorisations while supporting legitimate use of drones by industry, government, and recreational users.

Enhanced identification and tracking through conspicuity

Enhance drone operational accountability to support more effective monitoring, incident response, and risk analysis while minimising burden on legitimate users.

Balanced enforcement that deters misuse and enables innovation

Penalties and enforcement mechanisms to deter unlawful or dangerous drone operations while supporting legitimate use by industry, government, and recreational users.

Drone classifications and operating areas

New drone classifications, operating restrictions, and operational limits in areas where drone activity poses higher security risks. A risk-based approach would be applied to ensure adequate protections are in place without unnecessarily constraining compliant operators.

Build public and industry awareness

Raise public awareness of misuse related risks and relevant legislation, particularly around major events, critical infrastructure, and sensitive sites, to enable legitimate users to self-regulate drone use.

Proactive management of emerging drone threats

Regardless of drone types, reforms should enable timely detection, assessment, and mitigation by authorised counter-drone operators, who are supported by an adaptable regulatory framework that responds to new threat vectors as drone technologies advance.

A principle-based, policy framework that considers the broad use of drone technologies and takes an 'all-modes' approach will enhance national resilience particularly for protecting critical infrastructure. A policy framework that seeks to mitigate current gaps in aerial drone security, could be applied to address how drones increasingly operate in combined, cross-mode applications, such as maritime platforms launching aerial drones or land-based drones conducting reconnaissance for airborne systems.

A mode-agnostic framework will establish outcome-based security objectives that are future-proof in the face of ongoing technological advancements. Whether in the air, at sea, or on land, these systems rely on interconnected communications, position, navigation and timing systems (global navigation satellite systems; GNSS), various sensors, autonomy, software and remote command links each of which can be hijacked, spoofed, jammed, or manipulated by malicious actors.

Traditional physical security measures such as fences and standoff zones are ineffective when drones can fly, float or roll directly into restricted areas, bypassing conventional perimeter-based protections. This multi vector vulnerability demands an integrated approach where detection, tracking, and counter-drone authorisations apply to all system types, giving operators and governments a coherent defensive posture.

A mode agnostic drone policy framework offers clear advantages by addressing shared vulnerabilities across air, land and maritime systems and reducing regulatory gaps that could be exploited. However, prioritising reforms for aerial systems while embedding them within a broader, mode-neutral framework ensures that policy settings address the most pressing threats while still supporting a cohesive, future ready approach to unmanned technologies.

Questions:

- Are there specific risks you believe are unique to maritime or land-based drones that should be addressed differently within a national framework?
- How can a mode-agnostic, technology-neutral framework ensure legitimate commercial and recreational users are not unduly burdened while still mitigating security risks?
- Are there sectors that may face disproportionate impact from an all-modes approach, and how should government address these impacts?

Strengthened counter-drone capabilities to protect the community and infrastructure

Australia needs to enhance its capacity to detect, identify, mitigate, and counter malicious or unsafe drone activity by expanding counter-drone capabilities and authorisations. Measures would prioritise the protection of communities, critical infrastructure, crowded places (particularly at major events), and sensitive facilities while ensuring proportionality and minimising impacts to aviation safety.

Due to the speed of some drone technologies, response capabilities require real-time tracking and mitigation responses from regulators, law enforcement, security agencies and critical infrastructure operators to be effective.

Countering drone threats is a growing aspect of modern security planning. As drone use grows and technology becomes more advances, counter-drone approaches now require technologies, protocols, and strategies to detect, identify and prevent unauthorised drones from entering restricted or sensitive areas.

Many counter-drone technologies are based on manipulating the electromagnetic spectrum to interfere with how a drone is controlled. In particular, radiofrequency (RF) spectrum technologies that utilise jamming, including GNSS interference, can disable the drone while, in most cases ensuring the drone does not crash, avoiding harm to people and damage to property.

Drones are also able to be controlled by mobile phone and data networks and fibreoptic cables. At the same time, increasing autonomy, enabled by AI, means drones can perform their intended function without direct control by a person.

New or counter-drone capabilities are being developed. These include ways to take control of a drone, including via signal interception, as well as physical options such as lasers and interceptor drones. Counter-drone innovation and industry development is taking place in Australia, authorised via an exemption framework that allows for counter-drone research and development, manufacturing and testing.

When used without proper safeguards, active (transmitting) RF-based counter-drone capabilities can affect nearby frequencies, potentially impacting Wi Fi, mobile phone and data networks, GNSS, aviation navigation aids and aircraft onboard systems. The interference risks are increased for non-certified, unregulated, or low-quality counter-drone devices operated by unauthorised individuals.

Operational environments such as airports, ports, stadiums, and dense urban areas are particularly sensitive, because they host a complex mix of communication systems that depend on predictable and well-regulated RF behaviour. Small deviations from expected RF performance can also create operational challenges and put lives at risk. Therefore, reforms would continue to ensure that only properly authorised and trained operators deploy and manage counter drone technologies that impact RF.

The interdiction of a drone can also create safety risks, including the potential for collision with secondary objects, collateral interference with navigation systems, damage to infrastructure, or injury to people or property on the ground.

In light of these challenges, the Australian Government considers it necessary to ensure that law enforcement and security agencies have access to appropriate counter-drone tools and proportionate legal powers. Proposed reforms would strengthen existing capabilities to respond to unsafe or malicious drone activity while protecting public safety and critical systems.

These tools and powers would complement existing regulatory frameworks.

Questions:

- What safeguards or oversight do you think are important to ensure counter-drone technologies are used safely, proportionately, and appropriately?
- Who should be authorised (with appropriate training and approvals) to deploy drone detection or counter-drone technologies?
- What concerns do you have with expanded or additional counter-drone measures being introduced for authorised groups in Australia?
- What role should industry and the public play in reporting or helping to identify emerging drone threats?

Case study: European Union Counter-drone policy development

In September 2025, Denmark and Norway experienced a series of aerial drone incursions near major airports and critical infrastructure sites. These incursions caused widespread disruption to aviation operations, forcing temporary flight suspensions, delaying hundreds of services, and prompting heightened security postures across both countries. The incidents highlighted the growing vulnerability of civilian and industrial sites to hostile reconnaissance, service disruption, and malicious interference.

The North Atlantic Treaty Organisation increased its focus to create stronger defences against threat actors. The European Union accelerated work under its Defence Readiness Roadmap 2030. This initiative aims to strengthen preparedness across Europe against unmanned threats by improving detection, monitoring, and neutralising capabilities across member states.

A central feature is the concept of a ‘drone wall’. Rather than a physical barrier, the drone wall integrates sensors, radar systems, and signal jammers to provide continuous situational awareness.

These incidents underscored how fragmented counter-drone arrangements left individual countries exposed to cross border threats. By aiming for a fully operational drone wall by 2027, the initiative presents an integrated approach to safeguarding airports, energy sectors, and other critical infrastructure from the rapidly evolving risks posed by unmanned aircraft systems.

Enhanced identification and tracking through electronic conspicuity

Enhanced identification and electronic conspicuity technologies should be considered to improve operational visibility, accountability, and interoperability with security and safety systems. Approaches should support more effective monitoring, incident response, and risk analysis while minimising burden on compliant operators.

Reliable drone detection and operator accountability are essential to protecting critical infrastructure and ensuring the safe and secure use of emerging drone technologies. Without the capability to detect, track, and identify drones, authorities face a significant challenge in identifying malicious use and knowing where to act.

Many drones operate in ways that are difficult to detect using human senses and can be controlled remotely, making it challenging to identify the operator or their location. As a result, establishing a clear, real time electronic picture of drone activity has become a core security need for governments and operators of critical infrastructure and other sensitive sites.

Unidentified or untracked drones may be used for activities such as illicit surveillance, smuggling, interference with critical infrastructure, or intelligence gathering, and can also create safety and security concerns when operating near airports, energy assets, correctional facilities, defence sites, or crowded places.

For aerial drones, maintaining airspace accountability is essential to preserving situational awareness, ensuring compliance with regulations, and enabling timely enforcement when misuse occurs. The growing use of drones in maritime and land contexts pose similar challenges regarding compliance, situational awareness and enforcement.

Even well-meaning operators may inadvertently enter restricted airspace, disrupt emergency operations, or create collision hazards with crewed aircraft, vessels, or critical infrastructure. When a drone cannot be attributed to an operator, agencies lack the additional context necessary to determine whether the activity is benign, accidental, or potentially hostile. This uncertainty undermines confidence in airspace safety and limits the ability to respond effectively.

Under the current regulatory framework, only aerial drones used for commercial purposes are required to be registered with the Civil Aviation Safety Authority. To enhance Australia's airspace awareness, the Australian Government is also considering options for an expanded mandate for Automatic Dependent Surveillance-Broadcast (ADS-B) that includes options for aerial drones in certain circumstances. However, this technology is specifically designed to support safe air navigation and separation between other aircraft. It may not be the most effective technology option to provide awareness of drones for other purposes.

Taken together, these challenges highlight gaps in current identification and registration arrangements.

Further options to broaden the scope of drone operator accountability include additional electronic conspicuity to address gaps in drone identification and traceability. This would facilitate the identification of drones in-flight, and if coupled with solutions to capture operator details, would facilitate compliance action by law enforcement, national security and regulatory authorities.

Improved electronic identification and conspicuity would provide authorised and appropriately vetted entities with better situational awareness, enabling timely and informed responses to drone activity.
These capabilities would also support more accurate incident reporting by industry and infrastructure operators, improving information sharing with government agencies.

A range of detection systems and sensors are likely to be required to monitor drone activity for security, safety, and traffic management purposes. Given Australia's geographic scale, sharing drone detection data between government, commercial, and private entities may provide a cost-effective way to support real time responses to misuse, with appropriate safeguards in place.

Questions:

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

Balanced enforcement that deters misuse, and enables innovation

Penalties and enforcement mechanisms should clearly discourage unlawful or dangerous drone operations while supporting legitimate use by industry, government, and recreational users. The regulatory environment must maintain public safety while supporting economic and technological innovation.

To support the use of counter-drone capabilities and responses to drone misuse, there is a need to update Commonwealth and other jurisdictions law enforcement powers. This includes enabling appropriate information sharing from drone detection systems to support law enforcement, security, protection of critical infrastructure, aviation safety, and regulatory enforcement.

Addressing the legislative limitations of the current framework that only provides for enforcement relating to aviation safety issues, the initial phase of work, will support more effective management of the rapidly evolving risks of criminal and unlawful drone use. Legislation reform will also support better protection of public and crowded areas, critical infrastructure and improving the management of safety and environmental concerns related to the use of drones in Australia.

Updating legislative frameworks in line with the operating environment ensures that rules remain aligned with evolving capabilities. Establishing a legal framework that includes adaptable enforcement options such as tiered penalties and modern counter-drone tools and supports operational powers, will provide effective protections to respond effectively as threats evolve.

Complementing existing safety-related breaches, a tiered enforcement approach could deter misuse while remaining fair and proportionate. Lower level or unintentional breaches, such as accidentally flying in restricted areas without appropriate permissions, could be addressed through warnings, administrative penalties, or infringement notices to encourage compliance without being overly punitive.

More serious misconduct, including repeated negligence, reckless operations that endanger aircraft or emergency services, or deliberate misuse for surveillance or contraband delivery, could attract higher fines, licence suspension, or revocation of operating credentials. In the most serious cases, such as drone weaponisation, attempts to disrupt critical infrastructure, or activities linked to organised crime or terrorism, criminal penalties, including custodial sentences, may be appropriate.

Together, these measures would allow enforcement responses that are scaled according to risk, balancing deterrence with fairness while supporting responsible and legitimate drone use.

Questions:

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

Case study: Drone Drug Deliveries

In July 2020, Corrective Services officers stopped an attempted drone delivery of contraband into a correctional centre in the Hunter Region. The operation involved an aerial drone launched from a nearby vehicle and used to carry a package into the facility.

Officers later located the vehicle and seized the drone, which had a package attached containing prohibited substances. The incident occurred during the COVID 19 pandemic, a period when visitor restrictions led to an increase in attempts to introduce contraband through alternative methods, including drones.

The incident demonstrates how quickly criminal networks can adapt readily available technology for unlawful purposes and highlights the ongoing challenge for correctional facilities and law enforcement agencies in detecting and responding to emerging drone related threats.

Drone classifications and operating restrictions

Existing airspace architecture is designed around protecting the safety of aircraft and supporting air navigation. The use of airspace restrictions for certain sensitive sites may create a mechanism to allow authorities to quickly determine non-compliant drones, which would require new types of airspace categories. Some locations that are also accessible by drones that can operate on land or at sea may also require consideration.

Australia's current approach to restricted areas has mostly been built around safety, not security. While some locations already have protections, many high-risk sites fall outside existing rules.

As the use of drone technologies grows, whether for business, recreation, emergency services, or government work, Australia needs to think differently about how we manage and protect certain places. Some locations face higher security or safety risks when devices can move, fly, or operate remotely, and our current rules may not fully address these new challenges. These sites include:

- critical infrastructure (energy networks, water facilities, telecommunications assets)
- correctional centres
- hospitals and medical precincts
- government and research buildings
- major events and large public gatherings
- ports, rail corridors and other transport hubs.

Potential 'areas' that could be considered include the introduction of:

- permanent 'no go' zones around certain types of places
- restricted zones, where activity is allowed only under certain conditions
- enhanced monitoring zones, where activity is allowed but more closely tracked.

A stronger, more modern approach might include:

- more types of permanently restricted areas
- short term restrictions put in place during special circumstances
- zones with additional monitoring, where activity is still allowed but subject to extra oversight
- mandating digital rules are built into devices and updated automatically e.g. geofenced areas.

The Government is also seeking public views on how information about these zones should be best shared with operators. Risks can come from deliberate misuse, but many incidents also occur by mistake, for example, because a person is unaware of rules or their device's location. Either way, incidents can disrupt essential services, put people at risk, or interfere with emergency operations. This means Australia's approach to restricted area management needs consideration.

These options may become more practical when combined with other measures discussed in this paper such as technologies that can help identify, track, and manage activity more effectively.

As technology evolves, how Australia manages drone operations around sensitive or high-risk areas must remain agile and flexible. This includes looking at how permanent protections, temporary restrictions, and zones with additional monitoring can assist in keeping our community safe and secure.

Questions:

- Should specific no-use or enhanced-monitoring zones be designated around certain assets (e.g., hospitals, correctional and energy facilities)?
- What areas should be completely restricted from drone operations (unless approved)?
- How should ‘no-drone-zones’, or enhanced-monitoring zones be communicated, including to ensure proper coordination between enforcement entities and authorised operators?

Build public and industry awareness

Education and awareness campaigns should highlight drone related risks—particularly those affecting airspace, major events, critical infrastructure, and sensitive sites. Campaigns should promote responsible operation and improve public understanding of security obligations and safe operating rules.

Better education and guidance can reduce accidental misuse of drones, help prevent security incidents, and build public confidence in safe and legitimate use of drones. This is particularly important around sensitive locations such as major events, critical infrastructure, hospitals, correctional facilities, and defence sites, where even innocent mistakes can disrupt operations and place people at risk.

While the majority of drone operators are not malicious, recreational and well-meaning users can still create safety and security risks. The growing misuse of drones for activities including surveillance, smuggling, interference with critical infrastructure, and intelligence gathering highlights the need for targeted public awareness and education initiatives that reinforce operator obligations, lawful use requirements, and accountable operation.

Effective public education supports a culture of responsible operation by reducing accidental intrusions and strengthening operator accountability. Clear, accessible guidance helps operators understand and comply with requirements, reducing unintended breaches. It also helps law enforcement and security agencies distinguish between authorised and unauthorised drone operations and focus on genuinely harmful or reckless behaviour, supporting a safe and compliant operating environment.

What effective education could look like

To support safe and secure drone operations, the Government is exploring ways to make guidance easier to access and understand. This could include:

- **Public awareness measures –** Educate the public on security impacts of drone misuse, operating obligations, and potential penalties for misuse.
- **Partnerships with industry and hobby groups** – Work with manufacturers, retailers, and clubs to spread consistent messages on drone risks.
- **Counter-drone awareness –** Inform the public on counter-drone equipment, what it does, why it is used, and what might happen if they operate in the wrong place.

The proposed reforms would support consistent messaging on operator obligations, restricted areas, and counter-drone measures, reducing unintended breaches and enabling authorities to focus enforcement on genuinely unsafe or unlawful behaviour.

Questions:

- What information would help the public better understand risks associated with drones across land, air, and maritime domains?
- What communication channels or resources would make it easiest for operators to understand their responsibilities under a future all-modes framework?
- What public communication or education would help recreational and commercial operators avoid entering restricted airspace and understand their responsibilities?

Annexure A: What is a drone?

Drone Type	Description
Aerial	An uncrewed aerial system (UAS) is a complete set of components that together enable an aircraft to fly without a human on board. It includes the uncrewed aircraft itself, along with its control station, communication links, sensors, software, and any supporting equipment needed for safe and effective operation. These types of drones are the most common in Australia.
Maritime	Uncrewed maritime vehicles (UMV's) are autonomous or remotely operated systems that are traditionally used most by researchers and militaries. UMV's operate on water surface, and uncrewed underwater vehicles (UUV) operate under and on the water surface.
Land	Terrestrial drone technologies are uncrewed land-based robotic systems, designed to operate without an on-board human driver, using combinations of mobility, sensing, and communication systems, and autonomous navigation technologies to move across various terrains and perform tasks. These systems are considered separate to driverless cars and are less common than other modes in Australia.

Annexure B: Drone safety and security threats

Below are examples of impacts that drones may have if used maliciously.

Collision	The result of a drone deliberately or accidentally operating into an object (e.g. person, building or vehicle) causing financial loss, physical harm or death. Collisions can also be caused due to negligence, carelessness, or neglecting the controls of the drone.
Contraband Drop	The ability for an adversary using a drone to deliver items into a restricted area. These environments can include Immigration Detention Centres or across country and state borders. These items can include currency, narcotics, weapons, tobacco, alcohol, and digital devices.
Accident	The result of a drone losing control and crashing into infrastructure, people, or the ground.
Intelligence, Surveillance and Reconnaissance (ISR)	The ability for an adversary to use a drone with a variety of payload systems (cameras, Light Detection and Ranging (LIDAR), microphones, wireless capture) in order to capture information on a particular human or asset. Examples include spying on property or person before theft, spying on sensitive locations, or gaining valuable digital information.
Cyber Threat	Drone controlled by smartphones and other internet-connected devices can facilitate data egress and storage and enabling intelligence gathering While keeping network-connected devices updated is crucial for security, updates managed by foreign entities with interests separate to Australia could introduce hidden data collection capabilities, potentially accessible by the malicious actors through legal means. This may include broadening networks to access sensitive imagery, facility layouts, or other previously inaccessible areas. In addition to information gathering, unauthorised drone interference via remote take-over or unauthorised data extraction from an innocent user by a malicious user can also be of risk.
Restricted Area	The intrusion of a defined restricted area by a drone. The act of a drone in locations such as prisons, critical infrastructure facilities, airports, military installations, government buildings, etc. These locations can be defined by legislation, informed by the ground environment's specific application.
Strike	The ability for an adversary using a drone to perform an explosive, kinetic, liquid, hazardous materials (HAZMAT) or a chemical, biological, radiological and nuclear (CBRN) strike against a target. Payloads may be: • Attached to a drone for direct impact ("kamikaze" or "suicide"). • Attached to a drone for proximity impact (electronic or remote detonation). • Dropped from a drone for direct impact (often requiring a payload dropping mechanism).