Drone Security Public Consultation Response

Systra ANZ

Prepared for the Department of Home Affairs

25 May 2026

SYSTRA

Uncrewed Systems Policy Team
Uncrewed.systems.policy@homeaffairs.gov.au
Department of Home Affairs
Canberra ACT 2600

Via email

SYSTRA ANZ Submission on the Department of Home Affairs Drone Security Consultation Paper 2026

Dear Sir / Madam,

I write on behalf of *SYSTRA ANZ* in response to the Department of Home Affairs' *Drone Security Public Consultation Paper 2026*.

SYSTRA ANZ welcomes the Australian Government's focus on strengthening Australia's drone security framework in a way that protects communities, supports national resilience and enables the safe and productive use of emerging technologies. We support the Department's direction toward a *risk-based, proportionate and technology-neutral framework* that addresses malicious, negligent and unsafe drone activity while preserving legitimate commercial, government and recreational uses.

SYSTRA's perspective is informed by our expertise across *systems engineering, security, human/people factors, technology integration, transport and critical infrastructure resilience*. We work in complex, safety-critical and operationally sensitive environments where security, operations, people, technology and continuity of service must be designed and managed together. That perspective matters because drone security is not solely an aviation or law enforcement issue. It is also a matter of *systems assurance, infrastructure resilience, human performance, secure technology deployment and operational continuity*.

Our submission supports the overall direction of the consultation paper, including stronger counter-drone capability, improved identification and tracking, clearer operating restrictions around sensitive areas, and better public guidance. We also identify areas where the policy could be strengthened. In particular, we consider the framework would benefit from more explicit treatment of *critical infrastructure obligations and interfaces under the Security of Critical Infrastructure Act*, stronger recognition of *trusted technology, cyber and supply chain risks*, and clearer support for *tiered obligations* that scale according to risk, capability, location, human performance considerations and potential misuse.

SYSTRA's position is that Australia should seek to *maximise the benefits of drone technology while minimising and deterring misuse*. Lower-risk recreational activities should be supported through simple rules, clear education and designated areas of operation, while higher-risk activities near sensitive infrastructure, major events and transport assets should attract stronger requirements for identification, authorisation, monitoring and response. Effective policy should address not only technical controls, but also *the human elements that shape safe and secure outcomes*, including training, usability, decision-making, clarity of obligations and coordination between operators and authorities.

Please find attached SYSTRA ANZ's submission and supporting responses to the consultation questions. We would welcome the opportunity to discuss these matters further if that would assist the Department.

Yours sincerely

Andrew Waye
Executive General Manager - Security & Technology Solutions
SYSTRA ANZ

25 May 26

Contents

SYSTRA ANZ Response to Drone Security Consultation Paper 2026

Executive Summary

SYSTRA ANZ welcomes the opportunity to respond to the Department of Home Affairs' *Drone Security Public Consultation Paper 2026*. We support the overall direction of reform and the consultation paper's emphasis on balancing *security, public safety, innovation and community trust*.

SYSTRA supports the development of a drone security framework that is *risk-based, proportionate, technology-neutral and capable of evolving across aerial, land and maritime applications over time*. In our view, this is the appropriate policy architecture for an environment in which drone technologies are advancing rapidly and, as the consultation paper notes, capability is increasingly outpacing traditional regulatory settings.

Our perspective is informed by SYSTRA's expertise in *systems, security, human factors, technology integration, transport and infrastructure resilience*. We operate in complex operational settings where safety, security, continuity of service and secure-by-design outcomes must be considered together. We therefore approach drone security through a *resilience-by-design* lens: enabling beneficial use of drone technology while protecting critical assets, infrastructure systems and public spaces from disruption, misuse and harm.

SYSTRA also emphasises that *human factors are as important as technology settings* in achieving secure outcomes. Effective reform should therefore address not only device capability and enforcement powers, but also operator behaviour, usability of rules and systems, training, public understanding, supervision, communication and the design of interfaces and procedures that reduce the likelihood of error or misuse. In practice, this includes matters such as ensuring that no-drone alerts are presented clearly in operator apps, that approval pathways are usable in time-critical situations, and that detection interfaces support accurate decisions under pressure rather than creating unnecessary confusion or alarm overload.

SYSTRA supports the consultation paper's proposed policy development areas, including stronger detection and reporting capabilities, improved identification and traceability, clearer controls around sensitive sites, proportionate enforcement and stronger public guidance. We also recommend several areas for strengthening.

"Human factors are as important as technology settings in achieving secure outcomes."

First, the policy framework should more explicitly recognise the relationship between drone security and the *Security of Critical Infrastructure Act* environment. Drone misuse is not only an aviation safety or law enforcement issue; it is also a potential threat vector for critical infrastructure, operational technology environments and essential services. The final framework should align with broader approaches to critical infrastructure *risk management programs, incident reporting, resilience and continuity planning, and interdependency management*.

Second, reform should more directly address *trusted technology, cybersecurity, supply chain security, systems assurance and human factors*. As recognised in *Drone Security Public Consultation Paper 2026*, drones are connected cyber-physical systems. Risk can arise not only from malicious operators, but also from compromised platforms, insecure communications, vulnerable software, weak update management, poor interface design, inadequate training or unclear accountability.

Third, implementation should clearly adopt a *tiered model of obligations*. Requirements for registration, identification, approvals, monitoring and reporting should scale according to risk factors such as payload, autonomy, beyond-visual-line-of-sight operation, proximity to sensitive sites and potential for misuse. Recreational use in low-risk settings should not be burdened in the same way as higher-risk operations near critical infrastructure, major events, transport corridors, hospitals, correctional facilities or government assets.

Fourth, the framework should distinguish clearly between *passive detection and situational awareness* on the one hand, and *active counter-drone intervention* on the other. Broader access to detection capability may be appropriate for selected authorised users. Active mitigation powers should remain tightly controlled because of safety, communications, navigation, human decision-making and liability risks.

SYSTRA's overall position is that Australia should move promptly to modernise its drone security settings in a way that *maximises the good enabled by drone technology while minimising and deterring harmful uses*. The right framework will support innovation, productivity and operational efficiency, while strengthening resilience, trust and secure integration across systems, people and operations.

> ***SYSTRA recommends a stronger framework that aligns drone security with critical infrastructure obligations, addresses trusted technology and cyber risk, adopts tiered obligations based on risk, and clearly distinguishes passive detection from tightly controlled active intervention.***

Introduction

The Department of Home Affairs' *Drone Security Public Consultation Paper 2026* identifies a clear and growing need for reform. As the consultation paper states, drones are now part of everyday life in Australia and are increasingly used across business, government, emergency services, research, logistics, infrastructure and recreation. At the same time, drones can be misused to interfere with critical infrastructure, disrupt essential services, conduct unlawful surveillance, deliver contraband, or operate in restricted areas.

SYSTRA agrees with the consultation paper's core proposition that Australia's current framework has historically focused more on aviation safety than on drone-related security risks. While this approach has supported aviation outcomes, it does not by itself provide a complete response to the more complex security, infrastructure, cyber and operational challenges that have emerged as drone technology has become cheaper, more capable and easier to deploy.

"Drone security reform should therefore be approached as more than a narrow aviation policy exercise. It should be understood as a question of public safety, systems assurance, infrastructure resilience, cyber security, lawful use, human performance and secure technology integration."

Drone security reform should therefore be approached as more than a narrow aviation policy exercise. It should be understood as a question of *public safety, systems assurance, infrastructure resilience, cyber security, lawful use, human performance and secure technology integration*. This is particularly important in operational environments where failures or disruptions may create broader consequences across interconnected systems and services.

The consultation paper appropriately identifies six policy development areas: *proactive management of growing drone threats; strengthened counter-drone capability; enhanced identification and tracking; balanced enforcement; drone classifications and operating restrictions; and public and industry awareness*. SYSTRA supports this structure and offers this submission as a practical and strategic response to those areas.

About SYSTRA ANZ and Why Our Perspective Matters

SYSTRA ANZ is part of an international engineering and consulting group with deep experience in *transport, complex infrastructure, systems integration, safety, security and operational resilience*. In Australia and New Zealand, SYSTRA works across environments where infrastructure performance depends on the effective integration of people, process, technology and operations. Our expertise includes *systems engineering, security, human factors, operational technology, assurance and resilience-by-design*.

That perspective is directly relevant to this consultation. Drone security is not only a question of device regulation. It is also about how emerging technology interacts with complex operating environments, how risks are detected and managed across interconnected systems, how critical services continue to operate safely, and how human users understand and act within the framework. In other words, SYSTRA's perspective matters because we work at the point where *security, infrastructure, technology and human performance* intersect.

From that perspective, drones should be understood as both an *enabling technology* and a *potential threat vector*. Used appropriately, drones can support inspection, maintenance, surveying, emergency response, environmental monitoring, asset management and operational awareness. Used carelessly or maliciously, they can bypass traditional perimeters, create safety hazards, support hostile reconnaissance, disrupt transport and infrastructure operations, and undermine confidence in the secure management of public and critical assets.

This is particularly important in settings where infrastructure and services are interdependent. A drone incident near a rail corridor, station, tunnel portal, control facility, power asset, port interface, hospital precinct or major event location may create effects beyond the immediate incident area. These may include operational disruption, degraded maintenance access, public safety consequences, service interruption or increased security vulnerability.

SYSTRA's view is therefore that policy settings should be *systems-based, human-centred, proportionate and forward-looking*. The goal should not be to over-regulate a developing technology, but to establish clear and scalable guardrails that enable beneficial use while reducing opportunities for misuse and improving resilience.

SYSTRA's Overall Response

SYSTRA broadly supports the reform direction set out in *Drone Security Public Consultation Paper 2026*. The consultation paper appropriately recognises that Australia's regulatory framework must evolve to address negligent, unsafe and malicious uses of drone technology while preserving the value that drones can deliver across the economy.

SYSTRA supports, in principle:

- a *mode-agnostic and technology-neutral framework* that initially prioritises aerial drones but can evolve across land and maritime applications;
- stronger *detection, identification and tracking* capabilities to improve accountability and support proportionate enforcement;
- carefully governed access to *counter-drone capability* for authorised users;

a *tiered and proportionate enforcement model* that distinguishes between inadvertent, negligent, reckless and malicious conduct;

- clearer *operating restrictions and no-use or enhanced-monitoring zones* around sensitive locations; and

- stronger *public and industry awareness* to reduce accidental misuse and improve compliance.

SYSTRA supports the overall reform direction, with stronger emphasis on critical infrastructure alignment, trusted technology, human factors and practical proportionality.

At the same time, SYSTRA considers the policy should be strengthened in several areas.

The first is *critical infrastructure alignment*. The policy should more clearly link drone security reform to the *Security of Critical Infrastructure Act* environment, including the role of critical infrastructure risk management programs, incident reporting obligations, resilience planning and interdependency management. Drone misuse can be a vector for reconnaissance, disruption, contraband delivery, operational interference or cyber-enabled compromise affecting assets and systems of national significance.

The second is *trusted technology and supply chain assurance*. In higher-risk environments, security outcomes depend not only on operator conduct, but also on the integrity of the platforms, software, communications links and service providers involved. Reform should therefore more explicitly support secure communications, firmware and software assurance, trusted vendor approaches, update integrity, data governance and supply chain risk assessment for higher-risk use cases.

The third is *human factors*. Safe and secure outcomes depend heavily on how operators, responders, maintainers and regulators understand information, use systems, make decisions and coordinate action. A framework that is difficult to interpret, poorly communicated or operationally impractical will not achieve its intended outcomes, even if the technical rules are sound.

The fourth is *practical proportionality*. SYSTRA strongly supports a risk-based model in which controls scale according to risk. Lower-risk recreational activities should be addressed through clear rules, designated areas of operation and simple compliance pathways. Higher-risk activities involving sensitive assets, autonomy, payload, BVLOS operation or crowded places should attract stronger obligations.

Response to the Policy Development Areas

Proactive management of growing drone threats

SYSTRA supports a *mode-agnostic, technology-neutral and outcomes-based framework* that can respond to evolving risks across aerial, land and maritime drone applications. The consultation paper in *Drone Security Public Consultation Paper 2026* is correct to recognise that common security risks can arise across these domains, particularly where new capabilities enable cross-mode operation or allow malicious actors to bypass traditional controls.

However, while the framework should be common in policy design, implementation should be *tailored to operational context*. Maritime drones may raise particular concerns in ports, shipping channels, offshore energy environments and subsea assets. Land-based drones may create different vulnerabilities in transport precincts, depots, stations, logistics environments, tunnels and public access areas. Aerial drones remain the most immediate security priority, but future reform should avoid creating regulatory blind spots across other modes.

"SYSTRA supports a mode-agnostic, technology-neutral and outcomes-based framework that can respond to evolving risks across aerial, land and maritime drone applications."

A future-ready framework should address both *technical vulnerabilities and human-system interaction risks*, recognising that poor usability, unclear operating expectations and inadequate training can contribute to unsafe or non-compliant drone operations.

SYSTRA supports a national framework that sets consistent security outcomes while allowing differences in detection methods, operating rules, approvals and enforcement pathways according to the risk presented by the platform, operating environment and intended use.

Strengthened counter-drone capabilities to protect the community and infrastructure

SYSTRA supports strengthening Australia's ability to detect, identify and respond to unsafe or malicious drone activity. The consultation paper correctly identifies that effective response in many environments depends on *real-time situational awareness* and, in some cases, the ability of authorised entities to act quickly in order to protect communities, infrastructure and sensitive sites.

In SYSTRA's view, the reform framework should explicitly distinguish between *passive detection and situational awareness capabilities* and *active intervention capabilities*. Passive detection tools may appropriately be extended to selected critical infrastructure operators, emergency services, correctional facilities and major event operators where justified by risk and subject to standards, approvals and oversight. Such access can support early warning, incident reporting and better coordination with public authorities.

By contrast, active counter-drone measures, including jamming, signal interception, disabling or other forms of interdiction, should remain tightly controlled. As *Drone Security Public Consultation Paper 2026* notes, these capabilities can affect communications, GNSS, aviation systems and other critical technologies, particularly in airports, ports, stadiums, rail environments and dense urban areas. Active intervention should therefore be limited to properly authorised users operating under clear legal powers, competency requirements, technical standards, site-specific risk assessments and post-incident review obligations.

Safeguards should also address *human performance considerations*, including operator training, decision support, workload management, escalation protocols and interface design for detection and response systems. This is important because counter-drone decisions may need to be made quickly in complex environments, and poor human-system design could increase the risk of inappropriate intervention or unintended consequences.

Enhanced identification and tracking through conspicuity

SYSTRA supports stronger identification, traceability and electronic conspicuity settings for drones, especially in or near high-risk environments. The consultation paper correctly observes that current arrangements create gaps in the ability to identify drones and understand whether an operation is benign, accidental or potentially malicious.

In our view, effective drone identification is a foundational enabler for security, compliance and proportionate intervention. Authorities and other authorised entities should be able to access near real-time information about a drone's position, altitude, trajectory, device identity and, where legally justified and proportionate, relevant operator attribution. This visibility is particularly important near critical infrastructure, major events, transport assets, hospitals, correctional facilities and other sensitive sites.

> ***"In our view, effective drone identification is a foundational enabler for security, compliance and proportionate intervention."***

Identification and conspicuity measures should be designed not only for technical interoperability, but also for *operational usability*. Information presented to authorised users must be timely, understandable and actionable, so that operators and decision-makers can distinguish benign, accidental and potentially hostile activity without creating unnecessary false alarms or response burdens.

SYSTRA supports a *tiered model* under which registration and enhanced identification obligations scale according to risk. Factors may include payload, autonomy, beyond-visual-line-of-sight capability, operating environment, proximity to sensitive sites and use in higher-risk commercial or government operations. A broader range of technical solutions should be considered, including remote ID, network-based identification, telemetry sharing, secure authentication and multi-sensor detection approaches. As noted in *Drone Security Public Consultation Paper 2026*, a single universal technology may not be sufficient for all security purposes.

Balanced enforcement that deters misuse and enables innovation

SYSTRA supports a *graduated enforcement model* that distinguishes between inadvertent, negligent, reckless and malicious behaviour. The consultation paper is right to propose that enforcement should be strong enough to deter misuse while remaining fair and proportionate for legitimate operators.

"SYSTRA supports a graduated enforcement model that distinguishes between inadvertent, negligent, reckless and malicious behaviour."

In practice, this means that low-level or first-time breaches may be best addressed through warnings, education, administrative penalties or infringement notices. More serious misconduct, including repeated negligence, reckless operation near sensitive sites, interference with emergency services, or deliberate unlawful surveillance, should attract stronger penalties, including larger fines, licence suspension or revocation, and other regulatory sanctions.

In the most serious cases, including drone weaponisation, contraband delivery, hostile reconnaissance, attempts to disrupt critical infrastructure, or conduct linked to organised crime or terrorism, criminal penalties should be available. Enforcement responses should scale according to intent, risk and consequence.

Enforcement should also be complemented by *human-centred prevention measures*, including clearer user guidance, simpler compliance pathways, point-of-sale education, and better interface design in applications and devices. These measures can reduce inadvertent non-compliance and support more effective targeting of genuinely negligent or malicious behaviour.

SYSTRA also supports stronger reporting obligations for designated operators and entities that detect suspicious or unauthorised drone activity. Reporting should be standardised, risk-classified and supported by secure information-sharing arrangements so that higher-risk incidents can be escalated quickly and lower-risk events can still inform intelligence, trend analysis and future policy refinement.

Drone classifications and operating areas

SYSTRA supports stronger and clearer restrictions around locations where drone activity may pose heightened safety or security risks. The consultation paper appropriately identifies that Australia's historical approach to restricted areas has focused more on aviation safety than on security, and that many sensitive sites may not be adequately covered by current arrangements.

A stronger approach should adopt a *layered zoning model* comprising permanent prohibited zones, conditional access zones, temporary restrictions and enhanced-monitoring zones. This would allow controls to be scaled according to the sensitivity of the site and the legitimacy of the proposed operation. Such settings may be appropriate around correctional centres, hospitals, airports, defence sites, certain government facilities, telecommunications and energy assets, ports, rail corridors, depots, tunnels, emergency incident zones and major event precincts.

It is important that such restrictions remain practical and support approved legitimate use, such as emergency response, infrastructure inspection, authorised maintenance, and recreational use. Restrictions should therefore be risk-based, clearly justified and supported by workable approval pathways.

"Restrictions will only be effective if they are understandable and visible to operators in practice."

Restrictions will only be effective if they are *understandable and visible to operators in practice*. Human factors should therefore inform how approved zones, no-drone zones, conditional zones and alerts are presented across maps, apps, geofencing systems, signage and approval processes, so that users can easily understand what is required of them.

SYSTRA also supports the use of digital mapping, geofencing, machine-readable notices, operator applications, signage and coordination protocols to ensure restricted areas are clearly communicated and can be operationalised effectively.

Build public and industry awareness

SYSTRA supports stronger education and awareness measures as a core component of the reform package. The consultation paper in *Drone Security Public Consultation Paper 2026* correctly notes that many drone incidents are likely to involve careless or uninformed users rather than malicious actors. Better education can therefore reduce accidental misuse, improve compliance and help focus enforcement on genuinely harmful activity.

In our view, communication should be segmented by user group. Recreational users need simple, centralised and accessible guidance that helps them understand where they can fly, where they cannot, and why some locations are sensitive. Commercial operators and professional users require more detailed information about approvals, reporting obligations, identification requirements and operating restrictions in higher-risk environments.

Public education and awareness measures should be informed by *human factors principles*, including how people perceive risk, interpret instructions, respond to alerts and make decisions in real operating conditions. Guidance should be simple, consistent and accessible, with different communication approaches for recreational users, commercial operators and personnel working in sensitive or high-pressure environments.

There is also value in targeted communication at the point of sale, device activation and operator onboarding. Manufacturers, retailers, software providers, industry associations and regulators all have a role in helping users understand their obligations. For low-risk recreational use, designated flying areas and clear safe-use guidance may also assist in reducing unintentional breaches.

Additional Areas for Strengthening

Security of Critical Infrastructure alignment

SYSTRA considers the policy framework should more explicitly connect drone security reform to the *Security of Critical Infrastructure Act* context. The consultation paper appropriately identifies critical infrastructure as a core concern, but the policy would be stronger if it more clearly linked drone-related threats to the established critical infrastructure security architecture.

Drone misuse may be relevant to *critical infrastructure risk management programs, incident reporting obligations, resilience planning, continuity of essential services, and the management of interdependencies between physical, cyber and operational systems*. For example, drones may be used for hostile reconnaissance of asset layouts, operational interference at sensitive sites, contraband delivery, or collection of data that could expose vulnerabilities in essential systems.

SYSTRA does not suggest duplicating the SOCI framework within drone security policy. Rather, the two should be aligned so that drone-related threats and controls can be understood and managed within the broader infrastructure security and resilience environment.

Trusted technology, cyber security and supply chain assurance

SYSTRA considers that trusted technology and supply chain assurance should be more explicit features of the reform agenda. Security outcomes in higher-risk environments depend not only on operator behaviour, but also on the integrity of platforms, software, firmware, communications links, remote service pathways and supporting data environments.

For higher-risk deployments, especially those near critical infrastructure or involving sensitive operational data, policy should encourage or require consideration of *trusted vendor arrangements, secure software and firmware update processes, communications assurance, data governance, and supply chain risk assessment*. These issues become particularly important where platforms or service providers may be subject to offshore legal, technical or commercial arrangements that are not aligned with Australian security expectations.

This is consistent with the themes identified in *Drone Security Public Consultation Paper 2026*, which recognises cyber and supply chain risks as part of drone security, and it supports a more resilient and secure technology ecosystem over time.

Human factors, systems assurance and operational resilience

SYSTRA recommends that the policy framework more explicitly recognise the role of *human factors* in drone security and resilience. In practice, secure outcomes depend not only on technical controls, but on how operators, maintainers, responders and regulators interact with systems and information. User-centred design, training quality, cognitive workload, alarm management, communication protocols and clarity of procedures all influence whether a system is used safely and whether abnormal situations are recognised and managed effectively.

This is not an abstract issue. In practical terms, human factors can influence whether a recreational user correctly understands a no-drone alert before take-off, whether a critical infrastructure operator can distinguish a genuine threat from a benign contact on a detection screen, or whether an authorised responder can follow the correct escalation pathway in a time-critical situation. Embedding human factors into drone security policy would strengthen prevention, improve compliance and support more reliable operational response.

> ***"In practical terms, human factors can influence whether a recreational user correctly understands a no-drone alert before take-off, whether a critical infrastructure operator can distinguish a genuine threat from a benign contact on a detection screen, or whether an authorised responder can follow the correct escalation pathway in a time-critical situation."***

Taken together, these issues reinforce the importance of treating drone security as part of a broader systems assurance and resilience challenge, rather than only as a matter of device regulation.

Conclusion

SYSTRA ANZ supports the reform direction outlined in *Drone Security Public Consultation Paper 2026* and considers that Australia should move promptly to strengthen its drone security framework.

The strongest framework will be one that is *risk-based, proportionate, technology-neutral, human-centred and operationally practical*. It should support beneficial uses of drone technology while reducing opportunities for misuse, disruption and harm. It should also recognise that drone security is not solely an aviation issue. It is also a matter of *systems assurance, infrastructure resilience, cyber security, human performance, public safety and national security*.

SYSTRA supports the consultation paper's core policy development areas and recommends that the final framework be strengthened through clearer linkage to the *Security of Critical Infrastructure Act* context, stronger treatment of *trusted technology, cyber and supply chain risk*, explicit recognition of *human factors*, and more explicit *tiering of obligations and authorisations* according to risk.

"The strongest framework will be one that is risk-based, proportionate, technology-neutral, human-centred and operationally practical."

Australia has an opportunity to establish a modern, credible and future-ready drone security framework that maximises the value of drone technology while protecting communities, infrastructure, public confidence and essential services. SYSTRA would welcome further engagement as this policy develops.

Annex A – Responses to Consultation Questions

Policy Development Area 1

Proactive management of growing drone threats

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

Yes. Maritime and land-based drones introduce distinct operational, security and regulatory issues that should sit within a common national framework but be addressed through mode-specific controls.

Maritime drones may present particular risks to ports, shipping channels, offshore energy assets, subsea infrastructure, coastal surveillance environments and intermodal freight interfaces. In some cases, maritime platforms may also be used as launch points or support platforms for aerial systems, creating cross-mode threat pathways that conventional perimeter controls do not easily address.

Land-based drones may create different risks in public access areas, transport corridors, depots, logistics hubs, stations, tunnels, maintenance precincts and critical infrastructure sites. These systems can bypass conventional access control arrangements in ways that differ from aerial systems, particularly in constrained or mixed-use operational environments.

From a SYSTRA perspective, this distinction matters because operational impacts are highly environment-specific. For example, an aerial drone near a rail corridor presents one type of risk; a ground-based autonomous device entering a maintenance access route or station back-of-house environment presents another. A national framework should therefore be *mode-agnostic at the policy level* but *tailored in implementation*, including detection methods, operating restrictions, authorisation settings and enforcement pathways.

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

The framework should be *risk-based, proportionate and scalable*. Low-risk users and benign operations should face simple and low-cost compliance obligations, while higher-risk operations should attract stronger requirements for registration, identification, approvals, monitoring and competency.

For example, lower-risk recreational use could be supported through designated flying areas, clear digital guidance, point-of-sale education and simple operating rules. By contrast, operations involving sensitive sites, autonomous capability, payloads, BVLOS activity or use near critical infrastructure, major events, hospitals, ports, correctional facilities or transport hubs should attract stronger controls.

A technology-neutral approach should focus on outcomes such as *traceability, accountability, safe operating behaviour and resilience*, rather than locking in overly prescriptive technical requirements too early. It should also recognise that usability, operator understanding and clarity of obligations are important to compliance. This would reduce unnecessary burden on compliant operators while allowing the framework to adapt as technologies evolve.

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

Yes. Sectors such as transport, infrastructure inspection, logistics, construction, mining, agriculture, emergency services and research may face disproportionate operational or compliance impacts if controls are applied too broadly or without regard to context.

In many of these sectors, drones provide legitimate safety, efficiency and resilience benefits. For example, drones may reduce the need for personnel to enter hazardous locations, support asset inspections, improve situational awareness during incidents, or enable more efficient maintenance planning. These benefits should not be inadvertently constrained by overly general rules designed for higher-risk or malicious use cases.

Government should address these impacts through *phased implementation, sector-specific guidance, streamlined approvals for lower-risk professional use, and co-design with affected industries*. Guidance should also account for human factors, including the practical usability of requirements, clarity of responsibilities and integration with existing operational workflows.

Policy Development Area 2

Strengthened counter-drone capabilities to protect the community and infrastructure

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

Strong safeguards are essential. As recognised in *Drone Security Public Consultation Paper 2026*, radiofrequency-based counter-drone measures can affect Wi-Fi, mobile communications, GNSS and aviation systems. Their use should therefore be limited to authorised entities operating under clear legal powers, competency requirements, technical standards and approved procedures.

At a minimum, safeguards should include *defined operational thresholds, training and certification, site-specific risk assessments, equipment assurance, audit logging, incident reporting, post-use review, and clear accountability for decision-making*. Governance should also distinguish clearly between passive detection, tracking and identification functions, and active mitigation or interdiction functions.

Safeguards should also include *human factors considerations*, such as operator competency, recurrent training, workload management, clear escalation criteria, and user interfaces that support timely and accurate decision-making in high-pressure conditions.

This is particularly important in infrastructure-dense environments such as airports, ports, major event precincts, rail corridors, hospitals and dense urban areas, where even minor interference with communications, navigation or other operational technology may have disproportionate consequences.

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

Passive detection and situational awareness capabilities should be extended beyond law enforcement to selected additional user groups, including emergency services, correctional facility operators, designated critical infrastructure operators and major event security operators, subject to clear standards, approvals, training and oversight.

This reflects operational reality. In many environments, these organisations are the first to observe abnormal drone activity and are best placed to support early warning, local risk assessment and incident escalation.

However, active counter-drone capabilities that disrupt, disable, seize control of, or otherwise interfere with a drone should remain tightly restricted to authorised government agencies or specifically approved operators acting under strict legal and regulatory control. SYSTRA supports a *layered authorisation model* in which detection is more broadly available than intervention.

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

The principal concerns are unintended interference with communications and navigation systems, increased safety risks from forcing drones down or diverting them unpredictably, inconsistent operator competence, fragmented governance, and uncertainty around liability and post-incident accountability.

There is also a risk that intervention measures could affect legitimate drone operations if decision thresholds are unclear or if authorisations are too broadly distributed without consistent operational standards.

From a systems and infrastructure perspective, these concerns are material. Many high-risk environments already depend on tightly managed communications, control systems and safety protocols. Reforms should therefore avoid expanding intervention powers without equally strong governance, assurance and oversight arrangements. They should also account for the human elements of time-critical decision-making and the possibility of error under pressure.

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

Industry and the public should play a *structured supporting role*. Operators of critical infrastructure, transport precincts, major venues, ports, correctional facilities and other sensitive sites should have clear reporting pathways, escalation thresholds and data-sharing arrangements with authorities. They are often well placed to identify local patterns, recurring incidents, or unusual activity that may not be visible through centralised monitoring alone.

The public should be encouraged to report suspicious drone activity through simple and accessible channels, but should not be encouraged to intervene directly.

Industry can also assist through technical standards development, pilot programs, threat trend reporting, lessons learned from operational environments, and participation in trials of detection and information-sharing arrangements. This would support a more distributed and resilient approach to threat awareness.

Policy Development Area 3

Enhanced identification and tracking through conspicuity

What level of real-time visibility should authorities have to detect, track and identify drones operating near sensitive or high-risk environments?

At a minimum, authorised entities should have access to near real-time information on a drone's *position, altitude, direction of travel, speed and device identifier* when operating near sensitive or high-risk environments. Where legally justified and proportionate, operator attribution should also be available.

The level of visibility should scale according to the sensitivity of the site and the operational risk being managed. For example, a drone operating near a correctional facility, airport interface, energy asset, major event precinct, rail control environment or sensitive government site may justify a higher level of visibility than a drone operating in a low-risk recreational area.

The presentation of this information should also be *human-centred*. Data provided to authorised users should be clear, prioritised and operationally usable, so that decision-makers can interpret drone activity quickly and accurately.

SYSTRA supports a *risk-based attribution model* in which operator identity is available only to authorised entities and only where necessary to support timely and proportionate action.

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?

Detection equipment should be extended to selected additional user groups, especially emergency services, correctional facility operators, designated critical infrastructure operators and major event organisers, provided access is governed by standards, approvals, training, oversight and appropriate data controls.

The consultation paper in *Drone Security Public Consultation Paper 2026* recognises that a range of entities may need situational awareness of drone activity to manage security, safety and operational risks. SYSTRA agrees with this position.

However, access to *active mitigation or interdiction capability* should remain more tightly restricted than access to passive detection. The law and policy framework should make this distinction explicit.

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?

Registration and enhanced identification requirements should apply on a *tiered basis according to risk*. This may include drones above a defined weight, payload or capability threshold; drones used for BVLOS operation; autonomous or semi-autonomous platforms; drones used near sensitive sites; and drones used for higher-risk professional, commercial or government operations.

SYSTRA supports an approach that considers not only device size, but also *capability, context and potential misuse*. For example, a relatively small drone with advanced autonomy, camera payload or operation near a sensitive facility may justify stronger accountability measures than a larger but lower-risk device used in a controlled, approved environment.

A tiered model would avoid overburdening low-risk operators while improving traceability where the consequences of misuse or failure are greater.

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

Potential options include *remote ID, network-based identification, geofencing integration, telemetry sharing, secure operator authentication, and interoperable detection systems combining RF, radar, optical, acoustic and sensor-fusion approaches*.

As recognised in *Drone Security Public Consultation Paper 2026*, ADS-B may not be the most effective universal solution for security purposes. A broader and more flexible technology set should therefore be considered, particularly where different environments require different detection methods or where security outcomes depend on combining multiple data sources.

SYSTRA's view is that policy should focus on *interoperable, scalable and operationally usable situational awareness* rather than committing prematurely to a single technical architecture.

Policy Development Area 4

Balanced enforcement that deters misuse and enables innovation

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

A *tiered enforcement model* is appropriate and consistent with the approach outlined in *Drone Security Public Consultation Paper 2026*. Lower-level or unintentional breaches should generally be addressed through warnings, education, administrative penalties or infringement notices. This supports compliance without being unnecessarily punitive where risk or consequence is limited.

Repeated, reckless or high-risk misconduct should attract stronger penalties, including larger fines, licence suspension or revocation, and other regulatory consequences. Deliberate malicious use involving contraband delivery, hostile reconnaissance, disruption of infrastructure, interference with emergency operations, or weaponisation should attract criminal penalties, including custodial options where justified.

SYSTRA also supports the concept that enforcement should scale according to *intent, consequence, location and risk*. This preserves fairness while creating stronger deterrence around sensitive sites and malicious conduct.

What reporting obligations should apply when abnormal or unauthorised drone activity is detected, and how should information be shared with authorities?

Mandatory incident reporting should apply to designated critical infrastructure operators, airports, ports, correctional facilities, major event organisers and other approved operators where suspicious or unauthorised drone activity is detected in higher-risk environments.

Reporting should use *standardised formats, clear escalation thresholds and secure information-sharing channels* to law enforcement, aviation safety regulators and relevant security agencies. Data governance should be clearly defined, including privacy protections, evidentiary integrity, access controls, retention periods and role-based access to identification data.

Incidents should also be contextualised and assigned an appropriate risk classification. High-risk incidents involving suspected malicious intent, restricted area incursions, interference with operations, or threats to people and assets should trigger prompt escalation. Lower-risk incidents should still be captured where useful to inform threat intelligence, trend analysis and future policy development.

From a SYSTRA perspective, effective reporting arrangements are an important part of *resilience-by-design*: they support early awareness, coordinated response and continuous improvement across operators and authorities.

Policy Development Area 5

Drone classifications and operating areas

Should specific no-use or enhanced-monitoring zones be designated around certain assets?

Yes. A combination of *approved-for-use zones, permanent no-use zones, conditional restricted zones and enhanced-monitoring zones* should be designated around certain assets according to their sensitivity, operational context and the legitimate need for approved access.

Relevant sites include correctional facilities, hospitals and medical precincts, airports, defence sites, sensitive government facilities, energy and water assets, telecommunications infrastructure, ports, rail corridors, depots, major event precincts and emergency incident zones. This aligns with the policy intent in *Drone Security Public Consultation Paper 2026* and reflects the reality that some sites face elevated safety, security and continuity-of-service risks from drone activity.

A layered zoning model would allow Australia to manage risk more precisely than a binary authorised / unauthorised framework.

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

Areas that should generally be restricted unless specifically approved include correctional centres, defence facilities, active airport operating environments, certain critical infrastructure assets, emergency response zones, sensitive government sites, and major event venues during declared periods.

SYSTRA also considers that some transport and infrastructure environments may warrant stronger restriction settings depending on local risk. For example, rail control environments, tunnel portals, port security interfaces, or key asset maintenance precincts may justify restriction or enhanced monitoring where drone misuse could affect safety, continuity of operations or emergency access.

Restrictions should remain *risk-based, justified and operationally workable*, with practical approval pathways for legitimate users such as emergency responders, authorised inspectors, infrastructure maintainers or approved contractors.

How should no-drone zones or enhanced-monitoring zones be communicated?

These zones should be communicated through multiple channels, including *digital airspace maps, operator apps, manufacturer geofencing databases, machine-readable notices, approval platforms, signage at sensitive sites and direct coordination protocols for authorised operators*.

Information should be accurate, current, easy to understand and capable of automated integration where possible. This is particularly important for recreational and occasional users, who may not otherwise be aware of local restrictions, temporary controls or site sensitivity.

Education and communication materials should also be informed by *human factors principles*, recognising that compliance improves where restrictions are clearly presented, contextually relevant and easy to interpret in real operating conditions.

SYSTRA supports communication arrangements that combine public clarity with operational precision. Effective communication is essential both to reduce accidental breaches and to support enforceability.

Policy Development Area 6

Build public and industry awareness

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

Public guidance should explain *where drones can and cannot operate, why certain locations are sensitive, the types of harm drones can cause, penalties for misuse, and the difference between legitimate and unsafe use*. Practical examples are important, particularly around airports, hospitals, correctional facilities, major events, transport assets, critical infrastructure and sensitive government or defence sites.

It would also be helpful to explain, in plain language, that even relatively small or recreational drones can create disproportionate risk in the wrong environment. For example, a drone near a hospital helipad, rail corridor, energy site or emergency response area may create serious consequences even where the operator had no malicious intent.

For operators specifically, additional guidance should cover data sharing, privacy expectations, device capability, software assurance and obligations when operating near sensitive environments.

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

The most effective channels would likely include a *single authoritative government portal, mobile applications, manufacturer setup prompts, retailer information, operator accreditation materials, industry association guidance and targeted resources for infrastructure and commercial operators*.

For recreational users, it is sensible that CASA remain a key public-facing source of practical guidance, provided information remains consistent with the broader government framework.

SYSTRA supports a *segmented communication approach* in which basic rules are made highly visible for the general public, while more detailed operational guidance is provided for professional operators, infrastructure users and organisations operating in higher-risk settings.

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

Education should focus on *pre-flight awareness, digital mapping tools, mandatory onboarding information at point of sale or device activation, visual examples of restricted areas, major event alerts and simple explanations of approval pathways*. Public messaging should make clear that even unintentional misuse can create serious safety and security consequences.

For recreational users, designated flying areas, easy-to-use maps and simple "where you can fly / where you cannot fly" guidance are likely to be effective. For commercial and professional operators, additional education should address approvals, incident reporting, data sharing obligations, cybersecurity considerations and operating restrictions near sensitive assets.

Education materials should be designed using *human factors principles*, recognising that users are more likely to comply where information is timely, simple, contextual and aligned to real-world behaviour and decision-making.

From a SYSTRA perspective, effective education is not just a compliance measure; it is a means of supporting *safe adoption, operational resilience and informed use of emerging technology*.