



13 February 2025

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

By email: pjicis@aph.gov.au

Re: Review of the Transport Security Amendment (Security of Australia's Transport Sector) Bill 2024

The Australian Airports Association (AAA) welcomes the Australian Government's decision to send the Transport Security Amendment (Security of Australia's Transport Sector) Bill 2024 to the Parliamentary Joint Committee (the Committee) on Intelligence and Security for review. Representing over 340 airports across Australia—including major international hubs and smaller regional airports—the AAA advocates for the vital role that airports play in economic growth and community connectivity.

The AAA and its airport members fully grasp the importance of maintaining high standards in aviation security. Our members also understand the importance of the government ensuring that the legislation underpinning transport security remains fit for purpose, which necessitates updates to the legislation as this Bill intends to do. However, our members remain concerned about a number of aspects in relation to the Bill and are of the view that these concerns have not been adequately addressed or acknowledged by the Department of Home Affairs.

Regulatory Duplication and the All-Hazards Security Framework

The Australian Government is committed to ensuring that its agencies with regulatory responsibilities are aligned with RMG-128¹, its framework for ensuring they regulate according to its Best Practice Principles. These are:

1. Continuous improvement and building trust
2. Risk based and data driven
3. Collaboration and engagement

Under Principle 2, the Australian Government expects that "Regulators manage risks proportionately and maintain essential safeguards while minimising regulatory burden..."². One of the key pillars of the Bill is what the Australian Government has referred to as the "All-Hazards Security Framework". In response to the Department of Home Affairs' Transport Security Reform Consultation Paper (May 2024), AAA wrote to the Department on 21 June 2024 (see Appendix) highlighting that its then proposed "All-Hazards" was already addressed and regulated by Civil Aviation Safety Authority (CASA).

The Australian Government's Civil Aviation Safety Regulations (CASR) Part 139 of CASR Aerodromes allows CASA to mandate requirements for an airport operator's Aerodrome Emergency Plan (AEP) via the Manual of Standards (MOS), Part 139. Section 11.12 of the MOS Part 139 directs that an airport's AEP must include emergency arrangements, including procedures for emergency responses to natural hazards.

Chapter 24 of the MOS Part 139 states that an AEP must consider (among other things) "a full emergency", "other emergencies likely to present a hazard to an aircraft", which airports have assessed to include fire, road crash, storm events, aviation security incidents, hazmat, natural hazards (wind, hail, earthquake, flood, fire, etc.) and service disruption. Chapter 26 also addresses the risk management plans that airport operators are required to maintain.

¹ [RMG-128](#)

² RMG-128 [Principle 2](#)

Although this represents a clear example of regulatory duplication, the Department of Home Affairs has appeared to overlook this advice and continued to integrate it into its Bill. The AAA recently met with representatives from CASA's regulatory oversight team and were seemingly unaware of the Department's reforms and its potential to impact on one of the areas of airport operations that they already regulate.

The All-Hazards concept is not new³. It typically refers to a whole-of-government approach to the coordination and integrated response to the spectrum of risks that can threaten the well-being of communities and the broader society they aim to protect. This can include natural hazards, pandemics/public health, biosecurity, security (terrorism), cyber security/cyber attacks on critical infrastructure, supply chain resilience and so on. However, it is, for good reason, that specialist agencies have particular remits over natural disaster responses, pandemic response, security responses, public health responses etc.

Similarly, it is for good reason that specialists in each of these fields and their teams have oversight of these areas. At the same time, there is no question that there are times when a national, whole-of-government, coordinated response between agencies is necessary, just as there can be a need for a coordinated response at a local level.

In the Bill, the Department of Home Affairs calls for airport security teams to integrate the security response across:

- physical security
- personnel security
- cyber security
- supply chain security
- natural hazards

Natural hazards and their intersection with airports are already comprehensively regulated by CASA, as noted above, and remains best situated within emergency management frameworks.

Further, airports are already required to meet obligations under the SOCI Act (administered by Home Affairs) in relation to cyber security, making it unclear why there is a need for it to be included in the Bill or where Home Affairs' own regulatory approach under the SOCI Act in relation to designated airports will or will not overlap with it. As it stands, not only are designated airports already addressing cyber security obligations under the SOCI Act, many Tier 1 and Tier airports have already cyber security to their AEP frameworks as a standalone area or integrated under "Criminal Act" or "Sabotage". Additionally, the majority of Tier 2 and below airports are managed by local councils with IT departments that also specifically address cyber security obligations as part of shared services.

In the AAA's correspondence of 21 June 2024, we also raised concerns that placing supply chain security under the auspices of airports is unduly onerous as they extend beyond an airports area of operations. We proposed that the management of supply chain security is best situated with these critical service providers and regulated by Home Affairs in the same way that is under consideration for Regulated Air Cargo Agents (RACAs).

Recommendation 1: That the Committee review the Bill for regulatory overlap and duplication and eliminate it wherever possible.

Recommendation 2: That the Committee review the Bill to ensure the responsibility for supply chain security is situated with the service providers themselves, as this extends beyond the reasonable control of airports.

³ [WHO All-Hazard Definition](#)

Alignment with ICAO Standards and Recommended Practices (SARPs)

In reviewing what the Department of Home Affairs refers to as the All-Hazards Security Framework included in the Bill, the AAA reviewed ICAO's approach to Aviation Security for alignment. Australia has been a member state of ICAO since its establishment in 1944 following the signing of the Chicago Convention on International Civil Aviation. As a signatory and active participant, Australia is expected to comply with its ICAO's standards and recommended practices (SARPs).

The SARPs are published in the form of Annexes, of which CASA is responsible for 10 of the 19 Annexes⁴ in total (three of which are jointly shared with Airservices Australia (2) and the ATSB (1)). The Department of Home Affairs is responsible for one ICAO Annex, Annex 17 – Aviation Security. In the experience of AAA, the alignment between CASA's domestic rules and regulations is quite explicitly aligned with its respective ICAO Annexes. We cannot say this is also true of Home Affairs.

The AAA has reviewed Annex 17 – Aviation Security and found no reference to an All-Hazards Security Framework. In fact, there are no references to natural hazards in Annex 17 at all. However, natural hazards are covered in several other ICAO Annexes including, Annex 3 – Meteorological Service for International Air Navigation (BoM), Annex 6 – Operation of Aircraft (CASA), Annex 14 – Aerodromes (CASA) and, Annex 19 – Safety Management (CASA/ATSB).

As we highlighted in the previous section, CASA already regulates how airports integrate their safety response to natural disasters (and other hazards) in the Aerodrome Emergency Plans (AEPs) under CASR Part 139/MOS Part 139, which already addresses how natural hazards may impact on an airport and how the response should be managed. This is an obligation directly connected to its responsibilities under Annex 14 – Aerodromes and one where Home Affairs is not assigned an official role under its responsibilities.

As such, the AAA is of the view that the Department of Home Affairs' "All-Hazards Security Framework" is unaligned with the Department's obligations in relation to Annex 17. Consequently, it will create confusion, regulatory duplication and place an avoidable regulatory burden on airports.

Recommendation 3: That the Committee calls on the Department of Home Affairs to revise its "All-Hazards Security Framework" to eliminate the inclusion of natural hazards as it does not fall within ICAO Annex 17 – Aviation Security and is addressed elsewhere by three other government agencies.

Risk-based and Proportionate Regulations

As expected of the Australian Government's best practice regulatory principles outlined in RMG-128, the AAA and its airport members want to ensure that the reforms and areas that the Bill regulates in practice are risk-based. For example, it would be appropriate for the regulatory requirements to be linked to aircraft movements and passenger volumes. This would help to ensure that the regulations are proportionate and help to contain the cost of compliance for regional airports, again as we recommended in our correspondence of 21 June 2024. This is essential in ensuring that the Bill does not create an undue regulatory burden on the sector.

Airports have also raised concerns with us regarding the regulatory approach of Home Affairs, which can have a punitive focus rather than being more collaborative and educative. Airports take their security responsibilities very seriously and aim to comply with their obligations. A risk-based and proportionate approach to regulatory compliance would help to ensure that only the most serious breaches would warrant penalties being applied, not transgressions which present a relatively low risk and where collaboration and education could just as well yield the desired outcomes.

⁴ [ICAO Annex Responsibilities Australian Government Agencies](#)

Recommendation 4: That the Committee ensures that the Bill aligns with the Government's best practice regulatory principles so that it is risk-based, proportionate and does not create an unnecessary regulatory burden.

Recommendation 5: That the Committee ensures that the Department of Home Affairs also adopts a regulatory compliance approach that is risk-based and proportionate focusing on collaboration rather than punitive action.

Cost of Compliance Concerns

As noted above, it is critical that the regulations are implemented in a way that is risk-based and proportionate to ensure that the cost of compliance is not overbearing. It is already apparent that the legislation creates areas of regulatory duplication and overlap, which only add unnecessary regulatory burden and costs. The Department's own Impact Analysis for Final (First Pass) Assessment (which the sector was only provided 1 week to respond) incorporated modelling that showed costs to the sector of implementing the legislation approaching \$1 billion over the next decade. The cost of compliance here for just one area of regulatory compliance appears disproportionate.

As we highlighted in our response dated 24 October 2024 (see Appendix) this is not something that can be easily absorbed by large airports, let alone regional airports many of which are already running at a loss.⁵ The new security measures in the Bill could prove crippling for the sector, resulting in high airfare prices and lowering the commercial viability of certain routes.⁶

Recommendation 6: That the Committee ensures that the Bill does not create undue costs impacts on the airports sector as many airports are already cost-constrained.

Resourcing Constraints

As we highlighted in our correspondence to the Department of Home Affairs on 24 October 2024, the requirement for airports to undertake more extensive risk assessments and mitigation measures for a broader range of threats will place a considerable resourcing strain on airports. Airports have also raised concerns that with so many different regulatory frameworks already overlaid on their operational environment, this could actually result in impeding their ability to dynamically respond to a complex threat environment. It is critical that the Bill is reviewed to ensure that its implementation is practical and does not end up becoming counterproductive.

Recommendation 7: That the Committee reviews the Bill to ensure that it is practicable for airports to implement from a staff resourcing perspective.

Implementation Timeline

The Department of Home Affairs have previously indicated that airports would have 12 months to comply with the new legislative requirements. In the view of the AAA and its airport members, this is much too short a window for industry to ramp up its response and implement its new legislative obligations in full.

While the AAA and its members do not object to government regulatory regimes being enhanced over time, the current security arrangements have been effective, and we do not see why a longer implementation timeframe cannot be considered. Our preference is for an implementation timeline of at least 2 years as we have not been provided with any evidence that suggests the reforms need to be implemented sooner.

Recommendation 8: The implementation timeline be extended from 12 months to at least 2 years.

⁵ [Sustainability of Regional Airports](#)

⁶ [Security costs threaten services](#)

Formal Review of Legislative Implementation

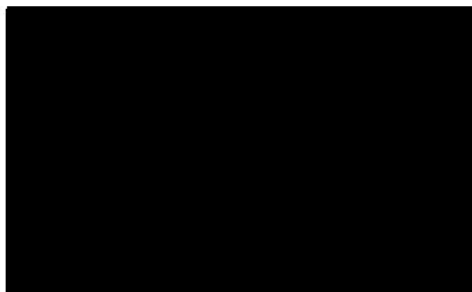
As part of the implementation process, we would also call on the Committee to direct the Department of Home Affairs to undertake a formal sector-wide review of the implementation process. This is to ensure that the implementation of the revised regulatory framework has indeed been successful in achieving its objectives and that it is not causing undue difficulties for airports. A formal review process within two years would allow for any adjustments to the regulatory framework so that any unintended consequences are identified with the certainty that they will be actioned in a timely manner.

Recommendation 9: A formal review of the implementation process to be undertaken within two years to ensure that the legislation is working as intended and to address any unintended consequences should these emerge.

We would like to thank the Committee once again for providing the opportunity to make a fresh submission in response to the Transport Security Amendment (Security of Australia's Transport Sector) Bill 2024. We understand the importance of continually improving the security arrangements in the aviation sector, but hope that these changes avoid regulatory duplication, are risk-based, proportionate and minimise the regulatory burden. Airports are already responsible for complying with a complex web of regulatory frameworks and any fresh layers need to be carefully considered and tailored so that they are fit for purpose.

For any further information about this submission, please contact [REDACTED] Senior Manager Regulatory Affairs on [REDACTED]

Sincerely,



Simon Westaway
Chief Executive
Australian Airports Association

Appendix

Appendix 1: AAA Submission to the Transport Security Reform Consultation Paper dated 21 June 2024

[Attached to the end of this document]

Appendix 2: AAA Submission to the Transport Security Amendment (Security of Australia's Transport Sector) Bill 2024 Impact Analysis for Final (First Pass) Assessment

[Attached to the end of this document]



AUSTRALIAN
AIRPORTS
ASSOCIATION

21 June 2024

Transport Security Reform Section
Critical Infrastructure Policy and Standards Branch
Industry Partnerships and Infrastructure Policy Division
Cyber and Infrastructure Security Group
Department of Home Affairs

Via email: [REDACTED]

Transport Security Reform Consultation Paper

The Australian Airports Association (AAA) is writing in response to the Department of Home Affairs (the Department's) consultation paper and supplementary paper (the Papers) dated 22 May and 30 May 2024, respectively, covering the Department's proposed Transport Security Reforms (the proposed Reforms).

The AAA represents the interests of more than 340 airports and aerodromes Australia-wide – from landing strips in remote communities to major international gateway airports. There are also 120 corporate members representing a broad range of firms providing goods and services to the airport sector.

There is a consensus among AAA members that the current regulations need updating due to the rapid evolution of aviation and technology and the significant and evolving threats of terrorism, espionage, foreign interference, and malicious cyber activity.

However, the AAA is concerned the Department's proposed reforms reflect a low threshold of ambition for genuine and substantive change to transport security arrangements, particularly after the thoroughgoing review led by Kerri Hartland in 2021-22 (the Hartland Review). The possibility of constructive change proposed in the Hartland Review has been shelved and replaced with a lower ambition 'patching' of the *Aviation Transport Security Act 2004* (ATSA) to bring the ATSA in line with the *Security of Critical Infrastructure Act 2018* (SOCI Act).

There is also a prevailing sentiment that the Department has sought only to inform the aviation and maritime sectors of its proposed approach rather than undertake genuine consultation. The Papers are seen as more advisory, as past consultations with the industry appear to have had a negligible impact on Departmental decision-making regarding the shape of the proposed Reforms. The proposals in the Papers closely mirror what was initially presented to the sector several months ago, suggesting that previous feedback may not have been fully considered.

Feedback in this submission from the industry on the proposed reforms contained in the Papers will focus on the Measures listed below:

1. **Unlawful Interference - Expand the definition of unlawful interference in ATSA and MTOFSA to capture a variety of acts and expand security incident reporting requirements.**

We acknowledge the increasing risk of cyber security threats and agree that the proposed reforms to the ATSA to incorporate cyber security should be considered a critical component of an airport's Transport Security Plan (TSP). However, expanding the reporting requirements to include attempted acts of unlawful interference of a cyber security nature presents significant challenges, mainly if information technology (IT) services are outsourced. This complexity is further exacerbated when the IT infrastructure is managed as part of a broader business, such as in council-owned and operated facilities.

Moreover, the proposed measures seem vague and broad, raising concerns that they could later be applied to a wide range of scenarios. In the past, vague regulations have created loopholes that inspectors and regulators have interpreted differently, leading to inconsistencies and compliance difficulties. The implications of this expansion need careful consideration, especially regarding the feasibility and practicality of meeting the enhanced reporting requirements.

Clear and precise guidelines are essential to avoid ambiguity and ensure all stakeholders understand their responsibilities and comply effectively. Assessing the feasibility and practicality of meeting these expanded reporting requirements is crucial, mainly when the airport does not directly control IT services and infrastructure.

2. All Hazards - Introduce all hazard security obligations under ATSA and MTOFSA.

Personnel Security - Requiring specific 'operational support' staff at an airport to undergo background checks and potentially obtain an Aviation Security Identification Card (ASIC) could be overly complex, mainly when a larger entity, such as a local council, may employ these staff. Moreover, using the ASIC for this purpose does not reflect the intended use of ASICs as stated in Section 3.03 of the *Air Transport Security Regulations 2005*.

Gateways controlled by individuals with ASICs would be a better approach, alongside reducing unnecessary access. This increased requirement for ASICs could strain AusCheck and the single issuing body model currently being implemented by the Department, which is already experiencing increased wait times for ASIC issuance.

Cyber Security - The cybersecurity proposals outlined in this section present significant challenges for airports regarding implementation and cost. From collective industry experience, it is observed that compliance with current cybersecurity frameworks, such as the Australian Signals Directorate's 'Essential Eight' Maturity Model, can be complicated and financially prohibitive. Many airports initially attempted to comply with the full suite of requirements but, due to complexity, were later re-evaluated to comply with only a subset of these controls. This adjustment underscores the substantial difficulty in achieving these standards.

Moreover, the requirement for an independent annual audit, which can cost around \$10,000 annually, further adds to the financial burden on airports. As several of the standards referenced in the proposals are U.S.-based, some concerns about adopting these standards might introduce further complexities and difficulties in achieving compliance. These standards might not be entirely suited to an Australian operational context and could impose additional burdens on airport resources. Given these considerations, the AAA urges the proposed reform to account for all airports' practical difficulties and financial implications. We recommend a phased approach or flexibility in compliance requirements to ensure these new cybersecurity measures are achievable and sustainable for the aviation industry.

Supply Chain Security - We understand the importance of enhancing supply chain security as outlined in the proposed Reforms. However, the examples provided, such as third-party security screeners and ground handlers, present significant commercial challenges for airports. Ensuring business continuity and redundancy measures with multiple providers could be difficult to manage and implement.

Given these challenges, the AAA proposes it may be more effective for these critical service providers to develop their own security and business continuity plans, regulated by the Department in the same manner that is now being considered for Regulated Air Cargo Agents (RACAs). This approach would ensure all critical service providers are equally accountable for their security measures, enhancing the overall resilience of the aviation sector without disproportionately burdening airports. Having these service providers directly regulated ensures a consistent and comprehensive approach to supply chain security.

Natural Hazards & All Hazards Risk Assessment and Attestation - While the AAA understands the importance of mitigating natural hazards, this measure seems inappropriate for inclusion under security regulations. Designated, Tier 1 and Tier 2 airports are already required to have comprehensive emergency management plans that address risks, hazards and threats specific to their location, as mandated by the Civil Aviation Safety Authority (CASA). Additionally, measures such as fostering infrastructure resilience and developing bushfire survival plans fall more appropriately under existing emergency management frameworks rather than security regulations. The AAA recommends any new requirements related to natural hazards be left with CASA and not included in any reforms to the ATSA or the Transport Security Regulations.

3. Security Controlled Activities Measure.

The proposed Security Controlled Activities (SCA) measures with additional background checks for specific individuals or requiring more personnel to hold ASICs could overwhelm the current system if additional resources are not allocated to ensure thorough and timely processing. In addition, this strain may lead to increased costs for obtaining ASICs, affecting both individuals and organisations financially. Leaving the determination up to Aviation Industry Participants (AIPs) to assess risk and decide on the necessity of an ASIC is a weak approach. It lacks consistency and could result in various industry security risk management standards.

As suggested in the consultation paper, introducing clear definitions and standardised criteria for SCAs would significantly improve this process. Such definitions would provide a uniform understanding of which roles and activities necessitate an ASIC, ensuring a consistent industry security approach. However, it complicates enforcement if IPs cannot compel third parties or employees to obtain an ASIC.

4. Amend the definition of 'test weapon'

The AAA supports this proposal and agrees with the Department's suggestion to broaden the definition. This will enhance the realism and comprehensiveness of security testing, improving aviation safety.

5. Introduce Vulnerability Testing

The AAA supports the implementation of vulnerability testing to enhance the overall security framework. However, we are concerned that this testing may become a mandatory compliance test component.

While vulnerability testing is valuable for identifying and addressing potential weaknesses within security systems, ensuring that such tests remain a tool for improvement rather than an additional compliance burden is essential.

7. Expand Special Security Direction Powers

While we support the proposal to expand the particular security direction (SSD) powers, these directives must be measured and proportionate. The industry should be thoroughly consulted to

ensure that the special directives will not have a detrimental impact on operations and that they are achievable within the operational constraints of airport management.

Although it is stated in the discussion paper that an SSD will be an extraordinary power used as a last resort, this principle needs to be explicitly articulated in the amended Act or Regulations. Codifying this principle will prevent misuse or overuse of power and ensure that it is not employed as an unthinking reaction to situations. This legislative clarity will assure industry stakeholders that SSDs will be issued judiciously and with consideration.

10. Alignment of Authority to Charge for Issuing a Security Identification Card Across the Transport Sector

The AAA supports aligning identification card fee structures across ASICs and MSICs. A standardised approach will reduce administrative burdens and ensure fair and transparent fee practices across the industry.

14. Replace 'Sex' With 'Gender', Where Practicable

The AAA supports this change in terminology to an updated and correct term. It reflects modern societal norms and is more appropriate for official documentation.

15. Remove the Term 'Fax'

The AAA agrees with removing outdated terminology. This modernisation will ensure the regulatory framework remains relevant and aligned with current communication technologies.

16. Exemption from State and Territory Requirements

The AAA agrees with and supports this measure, recognising the exemption of aviation security inspectors from state and territory licensing requirements. This will enhance the efficiency and effectiveness of system tests by increasing the pool of available inspectors and test items. This measure will help streamline operations and improve the responsiveness to changing threats.

17. Expand Who Can Conduct a System Test

While we have no serious issues with this proposal, consistency in testing practices and standards must be maintained if third-party providers are engaged. The AAA recommends ensuring the system test performance scorecard framework is uniformly applied across all airports to prevent discrepancies in the frequency and quality of tests. This consistency is essential for maintaining a fair and effective security testing regime.

18. Expand Compliance Control Direction Powers

The AAA seeks clarification on whether this measure extends to AIPs operating under commercial lease agreements within an airport's Transport Security Program (TSP). Currently, CISC's Civil Aviation Safety Inspector tends to hold the airport accountable for the actions of AIPs with airside access. The AAA believes compliance control directions (CCDs) should target the IPs responsible for their facilities to ensure accountability and fairness.

19. Introduce Infringement Notices for Unauthorised Access to an Airside Area of Secure Zone at a Security Controlled Airport

The AAA supports this measure and agrees that expanding the available regulatory enforcement options will assist in reducing costly and lengthy judicial proceedings and reflect a response to recent incidents of unauthorised airside access at airports.

20. Modernise the Security Program of Works

The AAA supports the initiative to modernise the security program framework. However, we have several concerns and seek further clarification on specific aspects of this measure.

The AAA and its members would like a clearer understanding of the outcome-focused framework that becomes enforceable under this measure. It is essential to ensure that CISC's Civil Aviation Safety Inspectors do not introduce new security requirements outside of established regulations, as this could lead to inconsistencies between states and territories. Uniform interpretation and enforcement of outcomes are vital to maintaining a consistent and coherent security framework across all jurisdictions.

This measure seems too general and lacks specific guidance. Further, more explicit guidance is needed to ensure all stakeholders understand expectations and requirements. Additionally, no time frames have been provided for when TSPs must be updated to incorporate these new measures. Clear timelines are essential to allow airports adequate time to comply with new requirements without disrupting operations.

By addressing these concerns and providing more detailed guidance and timelines, the modernised security program framework can be implemented effectively, ensuring enhanced security while maintaining operational stability across the aviation sector.

Other comments:

From consultation with its members, the AAA has identified significant concerns with the proposed Reforms contained in the Papers, with concerns listed as follows:

- A strong potential for 'doubling up' reporting requirements when managing 'all hazards' risks under the proposed Reforms. In any amending legislation, airports should be able to leverage their existing enterprise risk management programs and reporting protocols, replicating these systems through a revised TSP. The AAA recommends the Government could better manage 'all hazards' security outcomes through AIPs demonstrating alignment with accepted risk management frameworks (e.g., the 'Essential 8' for cybersecurity; AS 31000 for broader risk management) rather than requiring separate identification and mitigation processes for risks contained in an airport's TSP.
- The lack of boundaries for supply chain security measures is also an issue, with further potential for overlap and duplication of risk management requirements among AIPs. This is an issue for airports both forward and backward in their supply chain. For example, can offshore oil and gas platforms (as Systems of National Significance under the SOCI Act) submit an airport's TSP as an appropriate risk management instrument in their supply chain? Similarly, will the risk management instruments of goods and services providers in an airport's supply chain suppliers already covered in the SOCI Act (e.g., fuel, energy, communications) satisfy supply chain security measures under the proposed Reforms?
- Ensuring proposed Reforms are risk-based, with regulatory requirements for airports linked to aircraft volumes and passenger movements. Aligning the responsibilities of airports to manage risks under the proposed Reforms to the Department's tiered categorisation model for security-controlled airports would be a sensible and proportionate step in any draft legislation and help to contain compliance costs, particularly for regional airports.

Conclusion:

In conclusion, the AAA's view is the Australian Government's proposed reforms to aviation security should seek to balance policy and regulatory objectives within an efficient and flexible legislative framework, along with adequate incentives to encourage compliance where available, including:

- Support airports to meet their mandated requirement to upgrade aviation security screening of passengers and baggage.

- Ensure new aviation security legislation and regulation minimise the unintended consequences of inconsistent or overlapping regulation on security or compliance outcomes by the aviation industry;

The AAA welcomes the opportunity to provide feedback on the proposed reforms. If you require further information on issues raised in this submission, please get in touch with the AAA's Director of Airport Operations & Regulatory Affairs, [REDACTED]

Yours sincerely

[REDACTED]

Natalie Heazlewood

Head of Policy and Advocacy



24 October 2024

[REDACTED]
Avg Director | Transport Security Reform Team
Aviation Security Policy Branch | Critical Infrastructure Partnerships and Policy Division
Cyber and Infrastructure Security Group
Department of Home Affairs

Via email: [REDACTED]

Cc: [REDACTED]

Submission in response to the Transport Security Amendment (Security of Australia's Transport Sector) Bill 2024 Impact Analysis for Final (First Pass) Assessment

The Australian Airports Association (AAA) is writing in response to the Department of Home Affairs (the Department's) consultation paper "Transport Security Amendment (Security of Australia's Transport Sector) Bill 2024 Impact Analysis for Final (First Pass) Assessment."

The AAA represents the interests of more than 340 airports and aerodromes Australia-wide – from landing strips in remote communities to major international gateway airports. There are also 130 corporate members representing a broad range of firms providing goods and services to the airport sector.

Notwithstanding the tight turnaround of only one week to engage with our members and provide feedback in this latest phase of the consultation process, we acknowledge that feedback from stakeholders, including AAA, was adequately captured in the "Policy Approach Following Industry Consultation" document (September 2024) in response to the initial "Transport Security Reform Consultation Papers" (May 2024).

This included dropping the proposed requirement to have airports report all attempted cyber-attacks (Measure 1), which will limit the administrative burden to reporting actual security breaches. We also support the decision to expand the definition of "test weapon" to enhance the realism and comprehensiveness of security testing. It was also pleasing to see the transparency in the approach outlining how the policy position has shifted in response to stakeholder feedback and that modern regulatory principles have been factored into the development the First Pass Impact Analysis.

While we understand and support the need to enhance the security and resilience of Australia's transport sector, certain aspects of the proposed legislation have the potential to negatively impact the sustainability of the airports sector and further complicate the already complex regulatory environment in which they operate.

Cost of Compliance:

The compliance costs with the introduction of mandatory all-hazard security obligations, including cyber, supply chain, and natural hazard risk management are likely to be significant. Although the paper provides cost-benefit analyses, it does not fully accommodate for all the potential cost-implications the proposed changes at an operational level for airports. Unfortunately, this may not be fully understood until the specifics of the legislation and what exactly is being targeted is revealed. Yet, even without this

crucial information, the Department's initial cost estimates outlined in the Impact Analysis put the figures for airports at a substantial \$61 million in one-off costs with an ongoing cost of \$59 million per annum – and this is at the low end of the estimates. The high-end estimates provided could see these figures nearly double, with costs imposed on the sector approaching \$1 billion over the next decade.

This will have a costly impact on designated airports, especially as airlines are pushing back the on consistent increase of security costs. For regional airports, over half of which are operating at a loss¹, and struggling to get back to pre-Covid levels travel, the cost impacts could be crippling. With these airports unable to absorb the increased costs of compliance, these will inevitably be passed on to passengers, affecting the affordability and accessibility of regional air travel. Knock on effects of these cost increases across the aviation sector include less affordable air travel, potential impacts on employment, reduced productivity and efficiency of airport operations.

We have also seen the few carriers that support RPT routes balk at even minor cost increases that regional airports have passed on to customers to help fund the cost of regulatory compliance in the recent past², as these flow on effects can potentially jeopardise the commercial viability of these routes.

Resourcing Constraints:

We note that despite concerns previously raised about the impacts on resourcing of the proposed all-hazards approach, the Department's revised policy approach remains unaltered, with proposed mitigations largely centring on providing guidance. However, AAA remains concerned that the requirement for airports to conduct comprehensive risk assessments and implement mitigation measures for a broader range of threats will necessitate additional resources, both in terms of staffing and technology.

Many airports are already operating with limited resources, and the additional burden of these new obligations could have unintended consequences where other areas of security or safety may become compromised. With multiple legislative frameworks in play with significant regulatory overlap, the proposed changes will create an administrative burden that may also threaten the ability of critical infrastructure entities to remain dynamic enough to respond to a complex threat environment. We would ask that the government takes careful consideration when making their decision on these very important issues.

Implementation Timeline:

While we acknowledge the potential benefits of the proposed changes overall, including the need to properly align security-focus legislation affecting the sector, the proposed 12-month transition period for compliance with the new regulations may not be sufficient for many airports to fully implement the required changes. AAA is of the view that the complexity and scope of the new obligations necessitate a more extended period for thorough planning, resource allocation, and execution.

A 24-month phased implementation period may be more suitable, particularly for regional and smaller airports and to help industry better manage the new, and very substantial, cost impositions the new regime as outlined will impose. This would also offer an opportunity for feedback from the sector to the Department that may help it fine tune its guidance and support materials, as well as its regulatory

¹ <https://centreforaviation.com/analysis/reports/australias-regional-airports-will-be-unviable-without-federal-budget-aid-three-examples-examined-679056>

² <https://www.abc.net.au/news/2019-11-07/tensions-between-rex-airlines-dubbo-council-hit-new-highs/11682130>

approach to compliance – and indeed the coordination of the regulatory and compliance regime between agencies.

Additional Concerns:

Further, our members have put forward these questions for your consideration:

- Is the Department going to impose penalty units against certain aspects of the all-hazards approach?
- Noting that it is not part of the cost analysis, how would the all-hazards approach have prevented the examples provided in the Impact Analysis around the supply chain and natural disasters?
- For example, in the instance of cyclone Jasper, the paper mentions that more proactive measures would have supported the aviation sector in minimising supply chain issues (such as the flow on effects to critical emergency services) when it was rendered inoperable due to a natural weather event. Members would like to understand what this statement means and how an airport would proactively implement measures to mitigate this event?
- With an all-hazard approach, how would an airport mitigate for a measure that could contradict related legislation? For example, in an all-hazards approach, some members see the threat of PLAGs to a domestic flight the same risk as an international flight, however, current legislation does not allow airports to address this risk.
- What happens, for example, should an assessment conflict with the current legislation and an Aviation Screening Notice?
- Given the accelerated timeline for implementation of these reforms, how likely is it that this latest round of feedback will be properly considered and result in regulations that are proportionate, risk-based, and minimise the regulatory burden on airports?
- Will the regulations allow for the operational flexibility and sophistication that is an acknowledged strength of airports, or will they restrict their ability to respond appropriately because of the unintended consequences of red tape?
- Will the regulations support the stated objectives (p.5), and is a post-implementation review planned to identify if any of the proposed changes may require adjustment should they prove overly burdensome, restrictive and inefficient?

We appreciate the Department's commitment to enhancing the security Australia's transport sector on behalf of the Government and look forward to working collaboratively to achieve these goals in a way that does not place undue regulatory burden, cost and resourcing pressures on the airports sector.

Thank you for considering this critical issue. Should you require further information or clarification, please do not hesitate to contact [REDACTED] Senior Manager Regulatory Affairs via email [REDACTED]

Yours sincerely,

Natalie Heazlewood

Head of Policy and Advocacy

